Network Security Taskmanager

Benutzerhandbuch



Diese Software zeigt das Gefährdungspotenzial von aktiven Prozessen auf den Computern in Ihrem Netzwerk.

Inhaltsverzeichnis


Teil
I

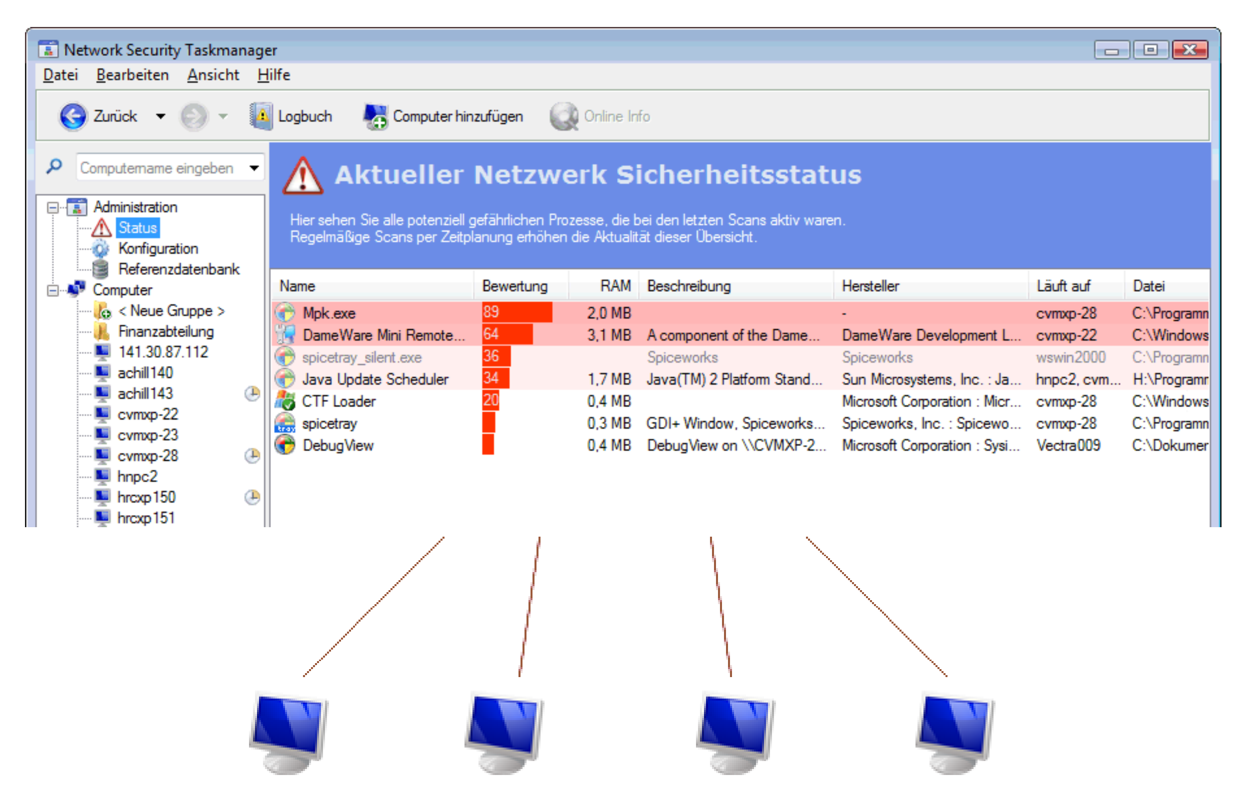
I. Willkommen

Network Security Taskmanager zeigt Ihnen alle aktiven Prozesse auf den Computern in Ihrem Netzwerk. Anhand der Bewertung 28 können Sie abschätzen, welche sicherheitskritischen Funktionen die Prozesse enthalten.

Network Security Taskmanager besteht aus zwei Komponenten:

Zentralkomponente

Die Management Console verwaltet zentral alle überwachten Computer. Der Administrator kann hiermit Computer scannen, Zeitpläne anlegen und Berichte ansehen.



Arbeitsplatzkomponente

Ein Software-Agent wird als Dienst auf den Computern gestartet. Auf Befehl der Zentralkomponente analysiert der Agent die aktiven Prozesse der Computer.

Einrichten

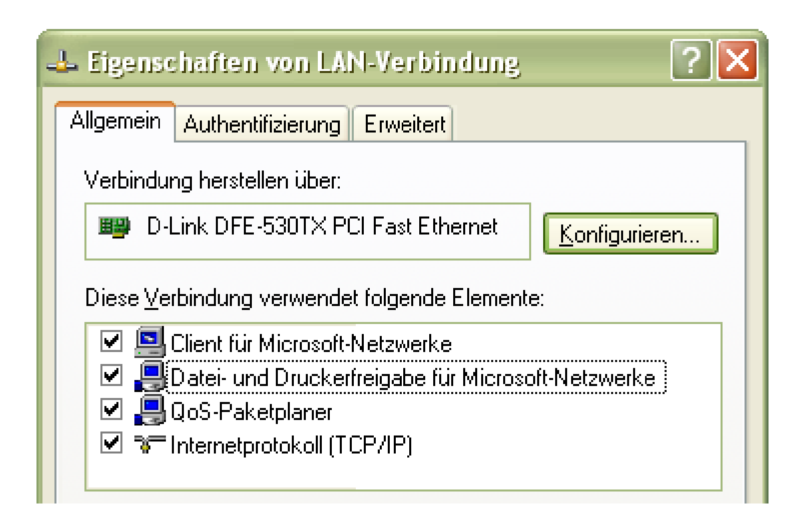


II. Einrichten

Systemvoraussetzung

Allgemein:

- Windows 8, 7, Vista, 2000, XP Professional, Windows Server
- Datei und Druckerfreigabe (standardmäßig aktiviert)
  Da *Network Security Taskmanager* das SMB Protokoll für die Kommunikation zwischen Zentral- und Arbeitsplatzkomponente verwendet, gilt auf allen Computern:
  - "Datei- und Druckerfreigaben für Microsoft-Netzwerke" aktivieren
  - Firewall Ausnahme für TCP Port 445 (Datei- und Druckerfreigabe)



Network Security Taskmanager funktioniert unabhängig von bereits vorhandener Sicherheitssoftware. Firewall oder Antivirensoftware anderer Hersteller müssen also nicht deinstalliert werden.

Zentralkomponente:

- ca. 4 MB Festplattenspeicher
  zzgl. 100 KB je überwachter Arbeitsplatzrechner

Arbeitsplatzkomponente:

- weniger als 1 MB Festplattenspeicher
- Admin-Freigabe Admin$ 32 aktiviert (standardmäßig aktiviert)
- falls Computer keiner Domäne angehört: Einfache Dateifreigabe 33 deaktivieren

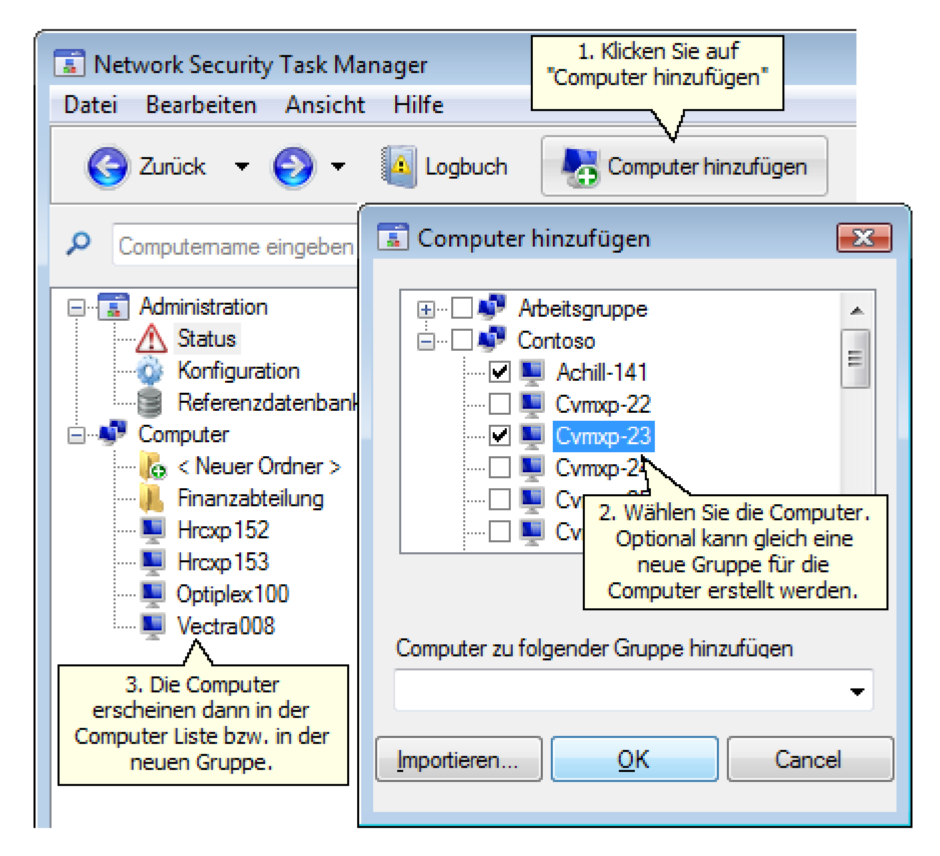
Hinweis: Wenn Sie mit dem Windows-Explorer wie folgt auf dem zu scannenden Computer zugreifen können, so funktioniert auch *Network Security Taskmanager*:



Installation der Zentralkomponente

Die Zentralkomponente kann unter jedem Benutzerkonto installiert werden.

1. Downloaden Sie die aktuelle Version von
   http://www.neuber.com/network-taskmanager/deutsch/download.html
2. Installieren Sie *Network Security Taskmanager*.
3. Öffnen Sie dann die Zentralkomponente
   (Start > Alle Programme > Network Security Taskmanager).
4. Klicken Sie auf **Neue Computer hinzufügen**.
   Hierbei werden die Computernamen in die Computer-Liste der Console hinzugefügt. Auf den Computern wird nichts installiert oder eingestellt.



Die Installation von *Network Security Taskmanager* ist damit abgeschlossen.
Sie können nun:

- Computer scannen 22,
- Computer in Gruppen zusammenfassen 12,
- Zeitpläne erstellen 15,
- sich bei potenziell gefährlichen Prozessen warnen lassen 17,
- vertrauenswürdige Programme als bekannt in die Refrenzdatenbank aufnehmen 18.

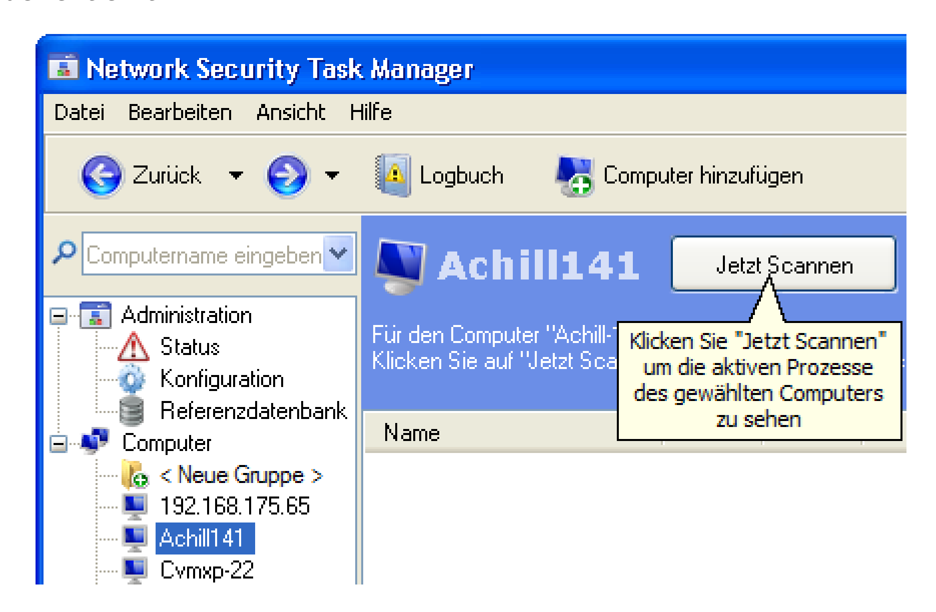
Anmerkung

- Die Zentralkomponente kann zusätzlich auf weiteren Computern installiert werden, um beliebige Clients manuell zu scannen. Auf diesen Clients darf jedoch von einer anderen Zentralkomponente keine Zeitplanung *Beim Start eines Prozesses* oder *Nach dem Booten des Clients* eingerichtet sein.
- Möchten Sie die Zentralkomponente aktualisieren, so installieren Sie einfach die neuste Version über Ihre vorhandene Installation.

Verteilung der Agenten

Sie brauchen sich um die Verteilung der Agenten in Ihrem Netzwerk keine Gedanken zu machen:

Wenn Sie mit Hilfe der Zentralkomponente einen Computer scannen, so wird automatisch ein Agent-Dienst auf diesem Computer installiert. Dieser Dienst analysiert die aktiven Prozesse und übermittelt die Daten verschlüsselt an die Zentralkomponente. Nach dem Scan wird dieser Dienst wieder entfernt.



Die Zentralkomponente installiert den Agent kurzzeitig in die Netzwerk-Freigabe „ADMIN$“ des gewählten Computers.

Mit einem Zeitplan [15] können Computer regelmäßig gescannt werden.
Bei den Zeitplanungs-Einstellungen *Beim Start eines Prozesses* und *Nach dem Booten des Clients* wird der Agent dauerhaft installiert. Wenn Sie diese Option wieder abwählen, so wird auch der Agent wieder deinstalliert.

Vorteil einer Zeitplanung: Im **Status** sehen Sie damit stets die aktuelle Sicherheitslage aller Computer.

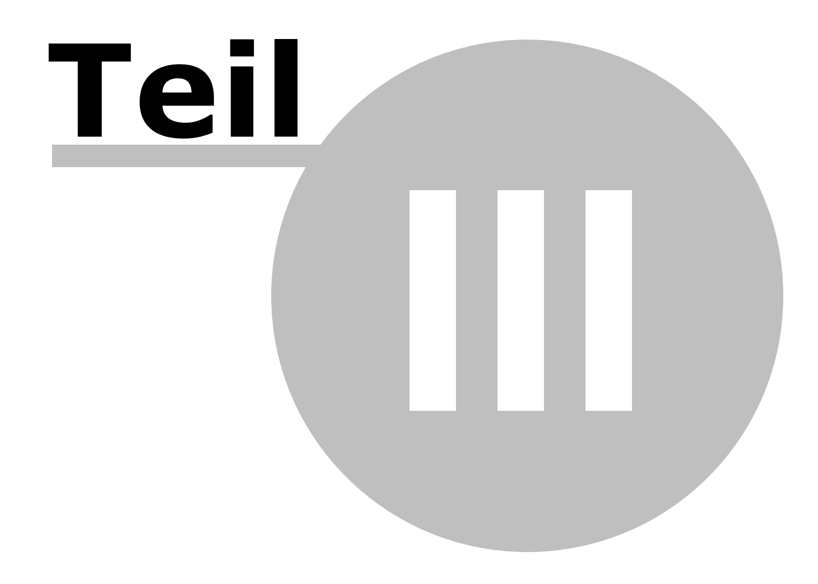


Name	Bewertung	Beschreibung	Hersteller	Läuft auf
MPK.exe	89	Mini Remote Control	-	vxp-23
spiceworks.exe	74	A component of ...	spiceworks	vmxp-28
KGB Monitoring	29	KGB Keylogger	-	vxp-23
spicetray		GDI+ Window, Spice ...	Spiceworks, Inc.	vmxp-28

Anmerkung

- Um Agenten auf einen Computer zu überprüfen, aktualisieren oder zu entfernen, klicken Sie mit der rechten Maustaste auf den gewünschten Computer. Klicken Sie nun auf **Agent-Dienst ▸**.
- Zur Verteilung der Arbeitsplatzkomponente in großen Netzwerken steht auch ein MSI-Paket [50] zur Verfügung.
- Der Agent benötigt nur 300 KB auf dem Arbeitsplatzrechner. Eventuell wird noch ein Cache bis zu 1 MB angelegt.

Konfiguration

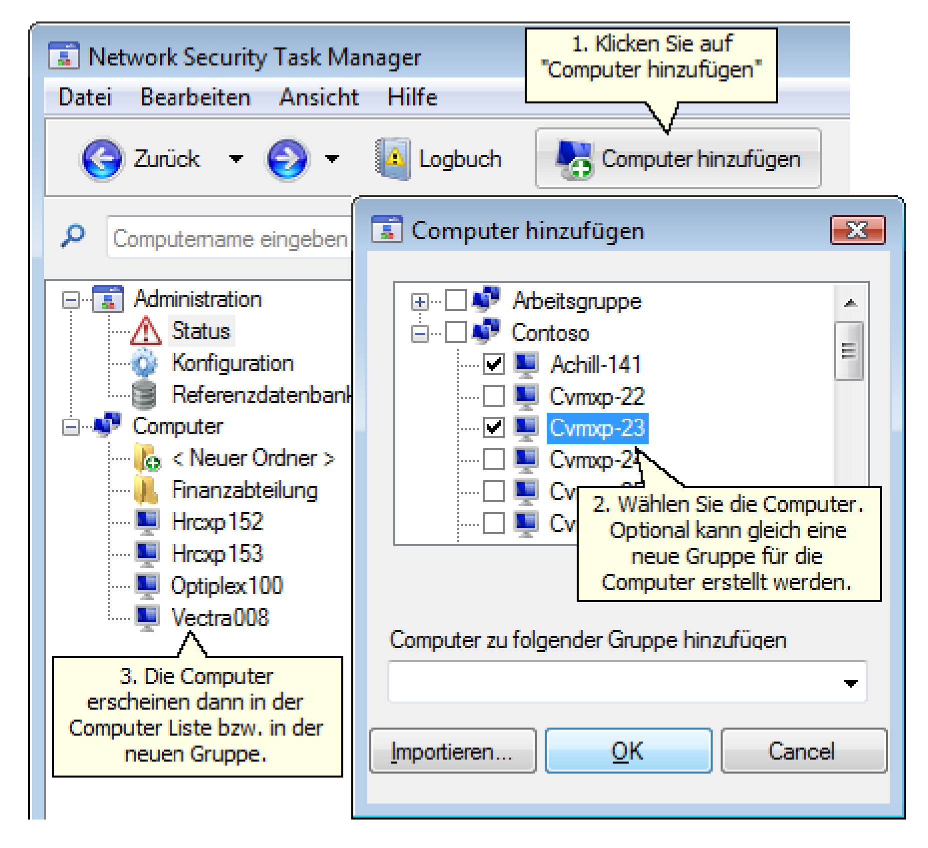


III. Konfiguration

Verwalten der Computer

Hinzufügen von Computern

Nach dem Start von Network Security Taskmanager sehen Sie alle Computer, welche Sie scannen können. Um weitere Computer hinzuzufügen, klicken Sie auf **Computer hinzufügen** in der Symbolleiste.



Alternativ können Sie auch im Feld Computername eingeben einen Computer oder dessen IP Adresse eintippen.

Auf den neu hinzugefügten Computern wird nichts installiert.

Die neu hinzugefügten Computer können nun von Ihnen manuell 22 oder regelmäßig per Zeitplanung 15 gescannt werden.

Anmerkung

- Klicken Sie auf **Importieren...**, um Computernamen aus einer Textdatei zur Computerliste hinzuzufügen. Jede Zeile sollte mit einem Computernamen beginnen. Nach einem Semikolon, Komma oder Tab-Zeichen stehende Texte bleiben unbeachtet.
- Nur auf Computern mit der Zeitplanung *Beim Start eines Prozesses* oder *Nach dem Booten des Clients* wird dauerhaft der Agent-Dienst installiert.
- Ein Computer kann gleichzeitig in verschiedenen Gruppen enthalten sein.

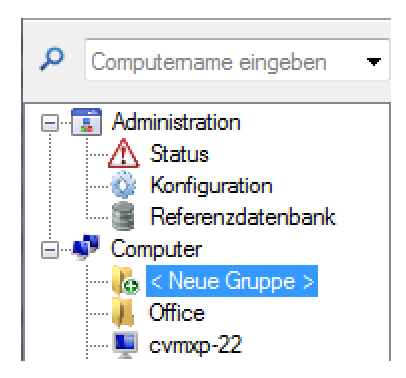
Zusammenfassen von Computern zu Gruppen

Sie können mehrere Computer zu einer Gruppe zusammenfassen. Für alle Computer dieser Gruppe gelten dann die gleichen Einstellungen, z.B. ein gleicher Zeitplan.

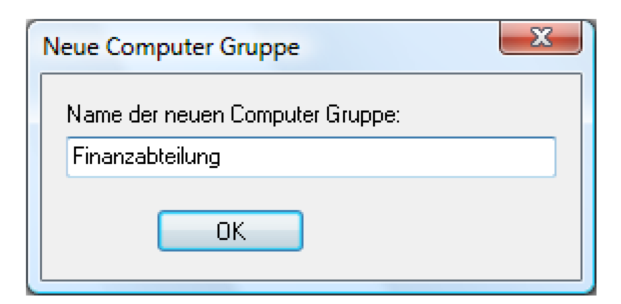
Gruppen können nach verschieden Auswahlkriterien gebildet werden. So können Sie alle Computer im gleichen Gebäude, mit gleichen Sicherheitsanforderungen oder analog der vorhandenen Active Directory Struktur zusammenfassen.

So erstellen Sie eine neue Gruppe

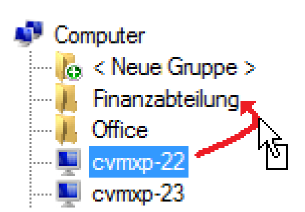
1. Klicken Sie auf **<Neue Gruppe>**.



2. Geben Sie einen bezeichnenden Namen für die Gruppe ein.



3. Ziehen Sie die gewünschten Computer auf die Gruppe.



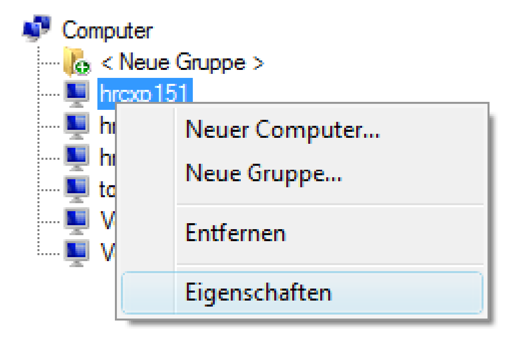
4. Um Computer zu einer Gruppe hinzuzufügen, die noch nicht in der Zentralkomponente aufgelistet sind, klicken Sie bitte auf **Computer hinzufügen**. Wählen Sie dann die neuen Computer und die gewünschte Gruppe.

Anmerkung

- Um eine Gruppe zu löschen, klicken Sie mit der rechten Maustaste auf diese. Klicken Sie anschließend auf **Entfernen**.

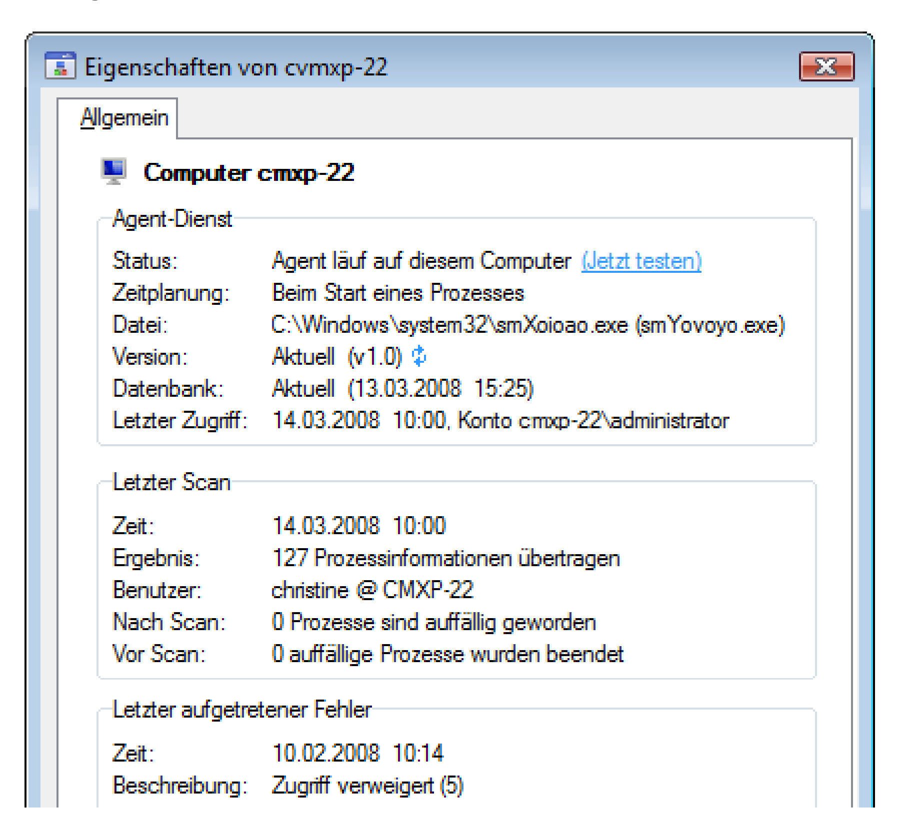
Anzeigen von Computer-Eigenschaften

Um alle Informationen über einen Computer zu sehen, klicken Sie auf diesen mit der rechten Maustaste auf diesen Computer. Klicken Sie dann auf **Eigenschaften**.



Sie sehen nun für diesen Computer:

- ob der Agent dauerhaft installiert ist,
- ob eine Zeitplanung eingestellt ist
- Datum und Ergebnis des letzten Scans

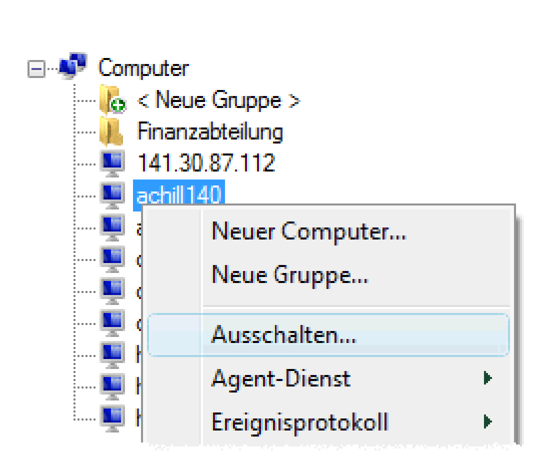


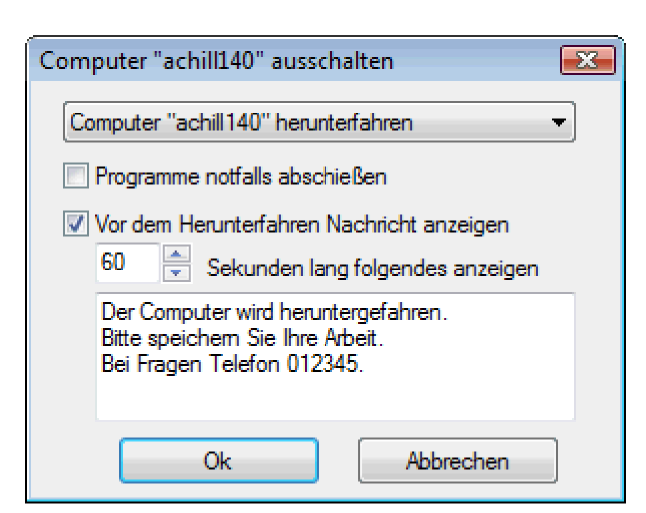
Anmerkung

- Bei der Zeitplanung *Beim Start eines Prozesses* oder *Nach dem Booten des Clients* wird der Agent Dienst dauerhaft auf einem Computer installiert.
  Klicken Sie auf neben der Versionsangabe, um die Agent-Datei zu aktualisieren.

Ausschalten eines Computers

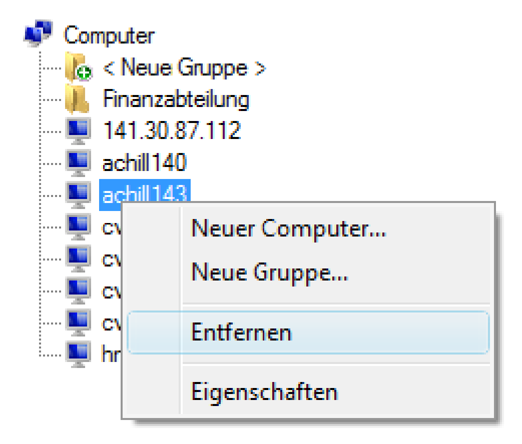
Um einen Computer auszuschalten, klicken Sie mit der rechten Maustaste auf diese. Klicken Sie dann auf **Ausschalten...**.





Entfernen von Computern

Um Arbeitsplatzrechner oder eine Computergruppe von der Computerliste der Zentralkomponente zu entfernen, klicken Sie mit der rechten Maustaste auf diese. Klicken Sie dann auf **Entfernen**.



Ist auf dem Computer der Agent-Dienst installiert, so wird dieser automatisch gestoppt und entfernt. Dies ist bei Computern mit der Zeitplanung *Beim Start eines Prozesses* oder *Nach dem Booten des Clients* der Fall.

Wenn auf dem Computer der Agent-Dienst per MSI-Paket 50 verteilt wurde, so sollte die Deinstallation auch per msi erfolgen. Also mit Ihrer Systemmanagementsoftware, Gruppenrichtlinien etc. pp.

Zeitplanung

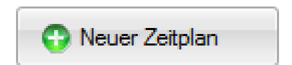
Network Security Taskmanager kann Computer oder Computergruppen automatisch zu bestimmten Zeiten scannen. Hierzu erstellen Sie einfach einen Zeitplan. Je Gruppe bzw. je (gruppenloser) Computer kann ein Zeitplan definiert werden.

So erstellen Sie einen Zeitplan

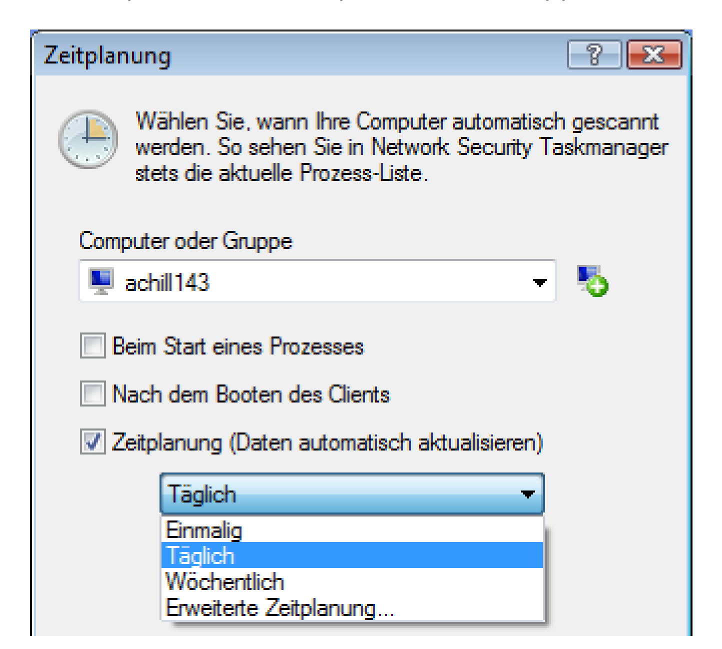
1. Klicken Sie auf **Konfiguration**.



2. Klicken Sie auf **Neuer Zeitplan**.



3. Wählen Sie den gewünschten Computer. Wenn Sie eine Computergruppe wählen, so gilt der Zeitplan für alle Computer dieser Gruppe.



4. Wählen Sie einen Zeitplan-Typ:

Beim Start eines Prozesses
Jeder neu gestartete Prozess auf dem Arbeitsplatzrechner wird überprüft (on access). Wenn der Prozess potenziell gefährlich 17 ist, so wird dies der Zentralkomponente gemeldet und der Administrator gewarnt.

Wenn Sie diese Option wählen, so installiert Network Security Taskmanager einen Agent-Dienst dauerhaft auf dem gewählten Computer. Der Agent-Dienst wird erst wieder deinstalliert, wenn Sie für diesen Computer eine andere Option wählen oder den Zeitplan löschen.

Nach dem Booten des Clients
Nach dem Booten des Computers werden alle aktiven Prozesse gescannt. So erkennen Sie insbesondere neue Autostart Programme.

Wenn Sie diese Option wählen, so installiert Network Security Taskmanager einen Agent-Dienst dauerhaft auf dem gewählten Computer. Der Agent-Dienst wird erst wieder deinstalliert, wenn Sie für diesen Computer eine andere Option wählen oder den Zeitplan löschen.

Einmalig
Der Computer wird zum gewählten Zeitpunkt von der Zentralkomponente gescannt. Hierzu wird kurz ein Agent-Dienst auf dem gewählten Computer installiert. Der Dienst scannt die zu diesem Zeitpunkt aktiven Prozesse und übermittelt die Ergebnisse verschlüsselt an die Zentralkomponente. Danach wird der Agent-Dienst wieder deinstalliert.

NetTaskTray 31 muss im Infobereich der Taskleiste aktiv sein, damit ein Computer zur vorgegebenen Zeit gescannt werden kann. Andernfalls (z.B. wenn der Network Security Taskmanager Benutzer zur Scanzeit nicht eingeloggt ist) erfolgt beim nächsten Network Security Taskmanager Start eine Abfrage, ob jetzt gescannt werden soll.

Täglich
Der Computer wird täglich zur eingestellten Uhrzeit von der Zentralkomponente gescannt. Hierzu wird kurz ein Agent-Dienst auf dem gewählten Computer installiert. Der Dienst scannt die zu diesem Zeitpunkt aktiven Prozesse und übermittelt die Ergebnisse verschlüsselt an die Zentralkomponente. Danach wird der Agent-Dienst wieder deinstalliert.

NetTaskTray 31 muss im Infobereich der Taskleiste aktiv sein, damit ein Computer zur vorgegebenen Zeit gescannt werden kann. Andernfalls (z.B. wenn der Network Security Taskmanager Benutzer zur Scanzeit nicht eingeloggt ist) erfolgt beim nächsten Network Security Taskmanager Start eine Abfrage, ob jetzt gescannt werden soll.

Wöchentlich
Der Computer wird wöchentlich am eingestellten Tag von der Zentralkomponente gescannt. Hierzu wird kurz ein Agent-Dienst auf dem gewählten Computer installiert. Der Dienst scannt die zu diesem Zeitpunkt aktiven Prozesse und übermittelt die Ergebnisse verschlüsselt an die Zentralkomponente. Danach wird der Agent-Dienst wieder deinstalliert.

NetTaskTray 31 muss im Infobereich der Taskleiste aktiv sein, damit ein Computer zur vorgegebenen Zeit gescannt werden kann. Andernfalls (z.B. wenn der Network Security Taskmanager Benutzer zur Scanzeit nicht eingeloggt ist) erfolgt beim nächsten Network Security Taskmanager Start eine Abfrage, ob jetzt gescannt werden soll.

Erweiterte Zeitplanung
Wählen Sie diese Option, wenn Sie die Zeitplanung individuell mit der Windows Aufgabenplanung (Zubehör > Systemprogramme > Geplante Tasks) einstellen möchten. Der Computer wird zum gewählten Zeitpunkt von der Zentralkomponente gescannt. Hierzu wird kurz ein Agent-Dienst auf dem gewählten Computer installiert. Der Dienst scannt die zu diesem Zeitpunkt aktiven Prozesse und übermittelt die Ergebnisse verschlüsselt an die Zentralkomponente. Danach wird der Agent-Dienst wieder deinstalliert.

Möchten Sie erweiterte Einstellungen vornehmen (z.B. monatlich, jeden 3. Tag oder unter anderem Benutzerkonto starten) so tragen Sie im Windows Task Planer ein:

```
"C:\xxx\NetTaskConsole.exe" "/scan:WinXP01"
```

oder

```
"C:\xxx\NetTaskConsole.exe" "/scan:WinXP01;WinXP02;Gruppe1;Gruppe2"
```

Im letzten Schritt des Windows Task Planers geben Sie bitte ein Benutzerkonto an, welches Admin-Rechte auf dem zu scannendem Computer besitzt. Damit kann die Zentralkomponente **NetTaskConsole.exe** den gewählten Computer scannen.

Anmerkung

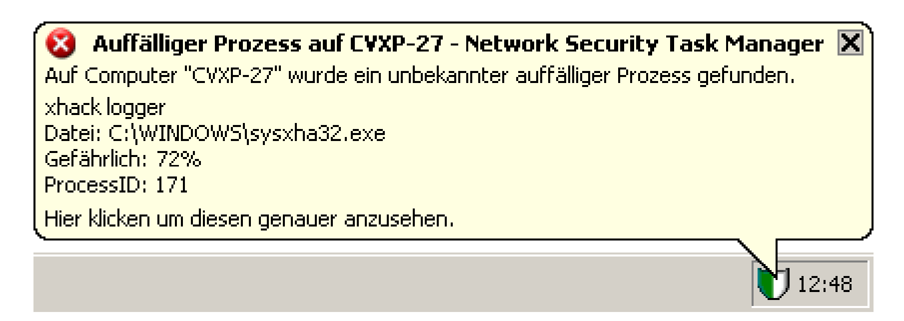
- Haben Sie in der Zeitplanung *Beim Start eines Prozesses* oder *Nach dem Booten des Clients* eingestellt, so muss auch auf dem Computer, auf dem die Zentralkomponente läuft, die Datei- und Druckerfreigabe aktiviert sein. Bei diesen beiden Zeitplänen wird die Zentralkomponente informiert 17, wenn ein potenziell gefährlicher Prozess gefunden wurde.
- Haben Sie in der Zeitplanung *Täglich/Wöchentlich/Einmalig* eingestellt, so muss NetTaskTray 31 in einem Benutzeraccount laufen, der Admin-Rechte auf dem zu scannenden Computerhat. Oder die Zentralkomponente läuft permanent.

Warnen bei gefährlichen Prozessen

Wird auf einem Computer im Netzwerk ein potenziell gefährlicher Prozess erkannt, so wird der Administrator auf verschiedenen Wegen gewarnt:

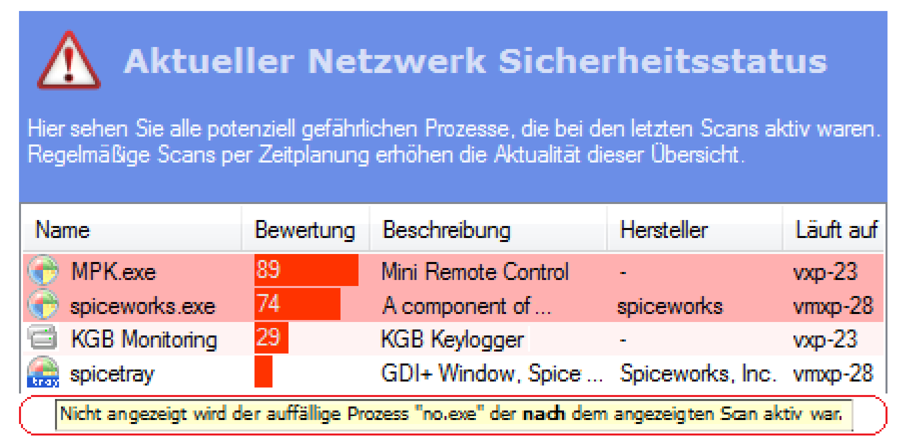
Popup Fenster auf dem Admin-PC

NetTaskTray 31 zeigt eine Warnmeldung als Popup-Fenster, wenn ein potenziell gefährlicher Prozess gefunden wurde.



"Status" Rubrik

Der Prozess wird im **Status** aufgelistet.



Name	Bewertung	Beschreibung	Hersteller	Läuft auf
MPK.exe	89	Mini Remote Control	-	vxp-23
spiceworks.exe	74	A component of ...	spiceworks	vmxp-28
KGB Monitoring	29	KGB Keylogger	-	vxp-23
spicetray		GDI+ Window, Spice ...	Spiceworks, Inc.	vmxp-28

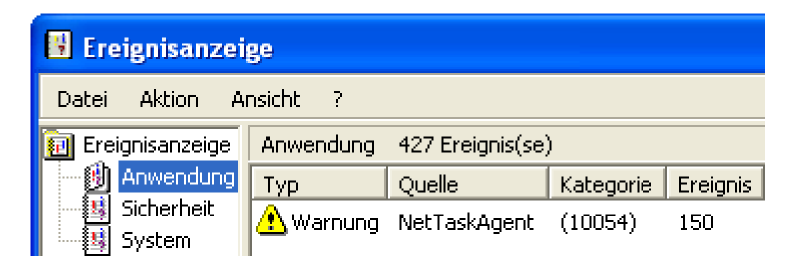
In der gelben Infozeile am Ende der Prozessliste wird auf potenziell gefährliche Prozesse hingewiesen, welche nach dem dargestellten Scan gestartet wurden. Diese Funktionalität steht nur zur Verfügung, wenn für den Clientcomputer die Zeitplanungsoption Beim Start eines Prozesses 15 eingerichtet ist.

Auffälligkeiten-Protokoll

Der Prozess wird in das Auffälligkeiten-Protokoll 25 (Logbuch) eingetragen. In diesem Protokoll sehen Sie alle in der Vergangenheit aufgetretenen Warnmeldungen.

Lokales Ereignisprotokoll des Clientcomputers

Der Prozess wird ins lokale Ereignisprotokoll des Arbeitsplatzrechners eingetragen und wird mit Ereignisanzeige eventvwr.exe oder Ihrer Systemmanagementsoftware angezeigt. Die Ereigniskennung lautet: 150



So legen Sie fest, ab welchem Risiko-Level der Administrator gewarnt wird

1. Klicken Sie auf **Konfiguration**.
2. Legen Sie im Bereich **Warnen** eine neue Risiko-Stufe fest.

   Warnungen

   Der Administrator erhält eine Warnung, wenn ein Prozess eine Risiko-Bewertung hat, die größer ist als: 70 %
   Prozesse mit einer höheren Risiko-Bewertung werden unter »Status« als sicherheitskritisch angezeigt.
   (0% = sicher, 100% = gefährlich)

   Alle Prozesse mit einer höheren Risiko Bewertung werden nun als potenziell gefährlich eingestuft.

Anmerkung

- Sie können einen Prozess als harmlos einstufen 19. Damit werden Sie in Zukunft bei diesem Prozess nicht mehr gewarnt.

Ausblenden von harmlosen Prozessen

Viele Prozesse machen eine Prozess-Liste schnell unübersichtlich. Deshalb ist es manchmal sinnvoll, folgende Prozesse nicht anzeigen zu lassen:

- Prozesse, die zum Windows Betriebssystem gehören
- Prozesse, die Sie persönlich in der Referenzdatenbank 18 als sicher eingestuft haben

So legen Sie fest, welche Prozesse nicht angezeigt werden:

1. Klicken Sie auf **Konfiguration**.
2. Legen Sie fest, welche Prozesse nicht angezeigt werden sollen.

   Ansicht

   Sie können sichere Prozesse in den Berichten ausblenden. Dieses verbessert die Übersicht.
   - [ ] Prozesse mit geringer Risiko-Bewertung (< 20%) ausblenden
   - [ ] Betriebssystem Prozesse ausblenden
   - [ ] Unverdächtige Referenzdatenbank Prozesse ausblenden

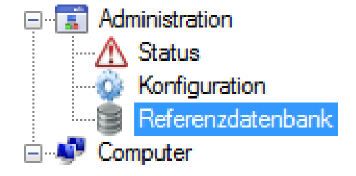
Anmerkung

- Wenn Sie Betriebssystem Prozesse ausblenden, so werden Applikationen wie explorer.exe trotzdem angezeigt.

Referenzdatenbank der bekannten Prozesse

Wozu dient die Referenzdatenbank?

In der **Referenzdatenbank** speichern Sie die Prozesse, die Ihnen bekannt sind. Jeden Prozess können Sie kommentieren und in eine der folgenden Risikogruppen einstufen:



Gefährliche Prozesse
können Schadsoftware (Spyware, Trojaner) oder auch unerwünschte Programme (Spiele, Adware, Filesharing) sein. Potenziell gefährliche Prozesse erhalten immer eine Risiko-Bewertung von 100 % (maximale Risiko-Klasse). Somit wird der Administrator immer gewarnt, wenn solch ein Prozess auf einem Arbeitsplatzrechner läuft.

Neutrale Prozesse
Sie haben zu diesen Prozessen einen Kommentar geschrieben. Diese Prozesse wurden aber von Ihnen nicht als *potenziell gefährlich* oder *ungefährlich* klassifiziert.

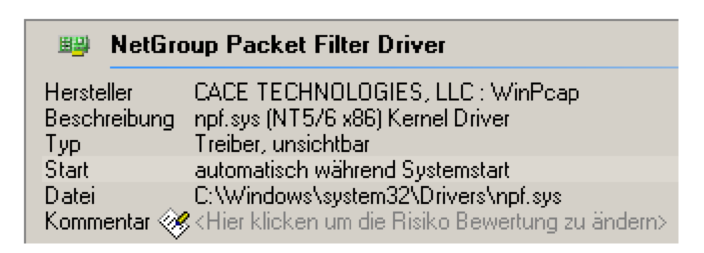
Ungefährliche Prozesse
sind z.B. Windows Systemprozesse, Grafikkartentreiber, Firewall, Viruswächter und andere vertrauenswürdige Programme. Klassifizieren Sie einen hoch bewerteten Prozess als ungefährlich, damit Sie zukünftig nicht mehr gewarnt werden, wenn der Prozess auf einem Arbeitsplatzrechner läuft.

Die Referenzdatenbank ist also eine Übersicht über alle Prozesse, welche Sie kommentiert haben oder dessen Risiko-Bewertung Sie geändert haben. Mit einer geänderten Risiko-Bewertung 28 werden Sie zukünftig *immer* oder *nicht mehr* gewarnt, wenn der Prozess gescannt wurde.

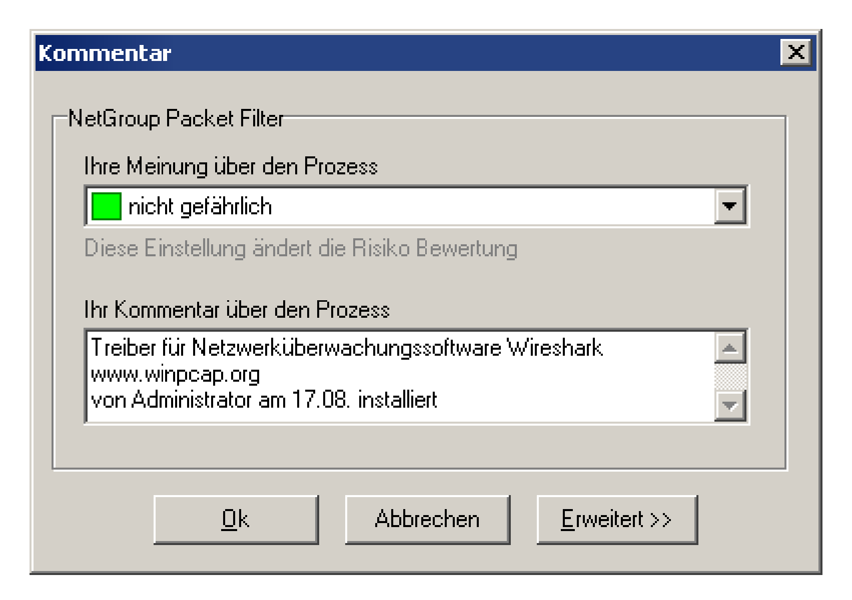
Hinzufügen von Prozessen zur Referenzdatenbank

Sie können beliebige Prozesse, welche Sie in der Prozessliste eines Computers oder einer Computergruppe sehen, zur **Referenzdatenbank** hinzufügen.

1. Klicken Sie auf den Prozess, welchen Sie in die Referenzdatenbank aufnehmen möchten.
2. Klicken Sie auf den roten Bewertungsbalken des Prozesses *oder* im unteren Teil des Programm-Fensters auf **Kommentar**.

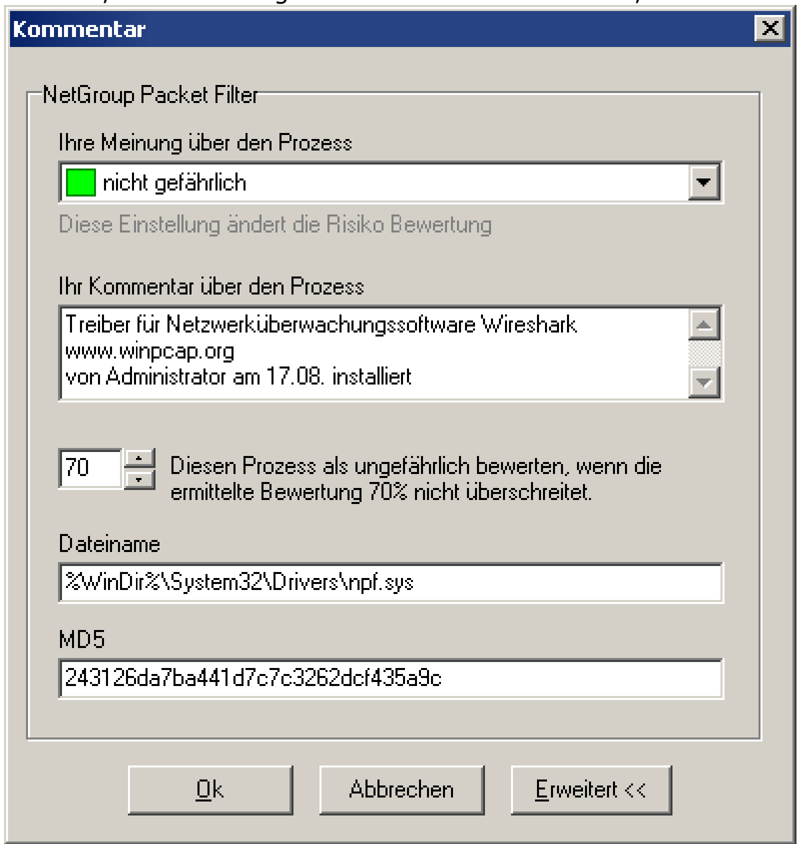


3. Geben Sie einen Kommentar (z.B. was Sie über den Prozess wissen) ein.



4. Optional können Sie den Prozess als neutral, gefährlich 18 oder ungefährlich 18 bewerten.
5. Klicken Sie auf **Erweitert**, um eine ganz bestimmte Risiko-Bewertung (z.B. 70 %) zu vergeben, bei der der Administrator gewarnt werden soll. Gefährliche Prozesse haben immer 100 % Risiko.
Sie können auch einen anderen Namen vergeben, mit welchem der Prozess in Zukunft angezeigt werden soll.

Network Security Taskmanager identifiziert die Prozesse anhand ihres Hash Wertes (eindeutige MD5 Prüfsumme). Wird ein in der Referenzdatenbank als harmlos eingestufter Prozess, durch einen gefährlichen Prozess ersetzt, so wird der Administrator gewarnt.



Anmerkung

- Möchten Sie immer gewarnt werden, wenn auf einem Computer z.B. die Datei *moorhuhn.exe* ausgeführt wird, so löschen Sie das Feld **MD5** und schreiben im Feld **Dateiname** nur: moorhuhn.exe
  Dies ist möglich, weil Prozesse per Dateinamen identifiziert werden, wenn das MD5 Feld leer ist.
- Filterreihenfolge: Gefährliche Datenbankeinträge überschreiben ungefährliche Datenbankeinträge.
- Sortierreihenfolge: Um den angezeigten Prozess- oder Herstellernamen zu ändern, klicken Sie bitte mit gedrückter Umschalttaste auf den Button "Erweitert >>".

Entfernen von Prozessen aus der Referenzdatenbank

1. Klicken Sie in der **Referenzdatenbank** mit der rechten Maustaste auf den Prozess, welchen Sie löschen möchten.
2. Klicken Sie auf **Entfernen**.

Anmerkung

- Wenn Sie einen Prozess in der Referenzdatenbank löschen, so löschen Sie "nur" Ihre Kommentare und Ihre Risiko-Einstufung zu diesem Prozess. Der eigentliche Prozess wird nicht angerührt.

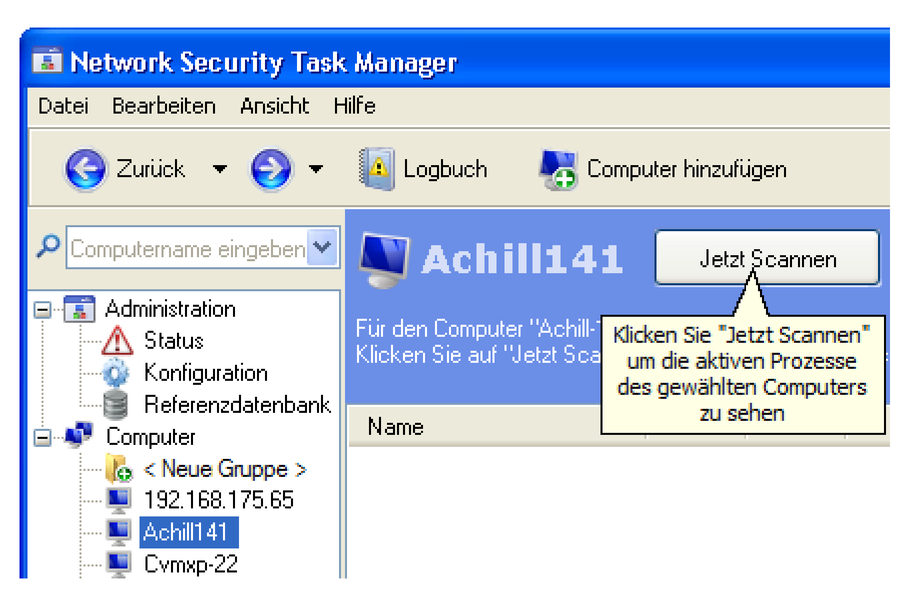
Arbeitsschritte



IV. Arbeitsschritte

Scannen der aktiven Prozesse auf einem Computer

1. Klicken Sie auf den Computer oder die Computergruppe, die Sie scannen möchten.
2. Klicken Sie auf **Jetzt Scannen**.



Anmerkung

- Sie können Computer und Computergruppen automatisch per Zeitplan 15 scannen.
- Um einen neuen Computer erstmalig zu scannen, geben Sie dessen Name oder IP Adresse im Feld Computername eingeben ein und drücken die Enter-Taste.

Speichern der Prozess-Liste

1. Klicken Sie im Menü **Datei** auf **Speichern unter...**
2. Wählen Sie als Dateityp:
   - Text file (*.txt)
   - Website (*.html)
   - All details (*.xml)

Anmerkung

- Klicken Sie auf **Konfiguration**, um sicher zu stellen, dass keine Prozesse ausgeblendet sind. Ausgeblendete Prozesse, z.B. Windows-Systemprozesse, werden nicht gespeichert.
- Speichern Sie die Prozess Liste von Zeit zu Zeit, um neue Prozesse ausfindig zu machen. Eine gespeicherte Prozess Liste kann auch für eine spätere Dokumentation nützlich sein.

Drucken der Prozess-Liste

1. Klicken Sie im Menü **Datei** auf **Drucken...**
2. Wählen Sie den Drucker und eventuelle Eigenschaften (z.B. beidseitiger Druck).

Anmerkung

- Klicken Sie auf **Konfiguration**, um sicher zu stellen, dass keine Prozesse ausgeblendet sind. Ausgeblendete Prozesse, z.B. Windows-Systemprozesse, werden auch nicht mit ausgedruckt.

Anzeigen von Prozess-Eigenschaften

Network Security Taskmanager zeigt Ihnen alle aktiven Prozesse auf den Computern in Ihrem Netzwerk.

Im Menü **Ansicht** können Sie wählen, welche Eigenschaften als Spalten in der Prozess-Liste angezeigt werden:

- **Name**
  Zeigt den Namen des Prozesses oder des Treibers an.
- **Bewertung**
  Zeigt, welche sicherheitskritischen Funktionen ein Prozess besitzt.
  0 % = sicher, 100 % = gefährlich
  Weitere Informationen 28
- **Clients**
  Zeigt die Anzahl der Computer in Ihrem Netzwerk, auf welchen der Prozess läuft. Ein Prozess wird anhand seines Hash Wertes (MD5 Prüfsumme) eindeutig identifiziert.
- **Läuft auf folgenden Clients**
  Zeigt die Namen der Computer in Ihrem Netzwerk, auf welchen der Prozess läuft.
- **Beschreibung**
  Zeigt den Titel und die in der Datei enthaltene Datei-Beschreibung. Bei einem sichtbaren Fenster entspricht der Titel dem Text in der Titelleiste.
- **Hersteller**
  Zeigt den Namen des Herstellers (z.B. Microsoft) und die in der Datei gespeicherte Produktbeschreibung (z.B. MS Office). Damit erkennen Sie zu welchem installierten Software-Produkt ein Prozess gehört.
- **Datei**
  Zeigt den kompletten Pfad und den Namen der Datei.
- **Durchschnittliche CPU Laufzeit**
  Zeigt die Inanspruchnahme des Prozessors. Aktive Programme benötigen mehr Prozessorleistung als inaktive Prozesse.
- **Durchschnittlicher RAM auf allen Clients**
  Zeigt den Arbeitsspeicher-Verbrauch eines Prozesses.
- **Durchschnittliche Laufzeit auf allen Clients**
  Zeigt die Zeit, in der das Programm seit dem Windows-Start aktiv gearbeitet hat.
- **Prozess ID (PID) des am höchsten bewerteten Prozesses**
  Zeigt die Identifikationsnummer (ID) des Prozesses. Jeder Prozess besitzt eine eigene, eindeutige Nummer.
  Läuft der Prozess auf mehreren Computern, so besitzt er auf jedem Computer eine andere PID. Alle PID's sehen Sie in dem Sie auf den Prozess doppelt klicken.
- **Typ (Programm, Treiber, Dienst, PlugIn, ...)**
  Zeigt die Art des Prozesses an. Es wird zwischen verschiedenen Prozess-Typen unterschieden.
  Weitere Informationen 30
- **Start Information des Prozesses**
  Zeigt wann und durch wen der Prozess gestartet wurde.

Anmerkung

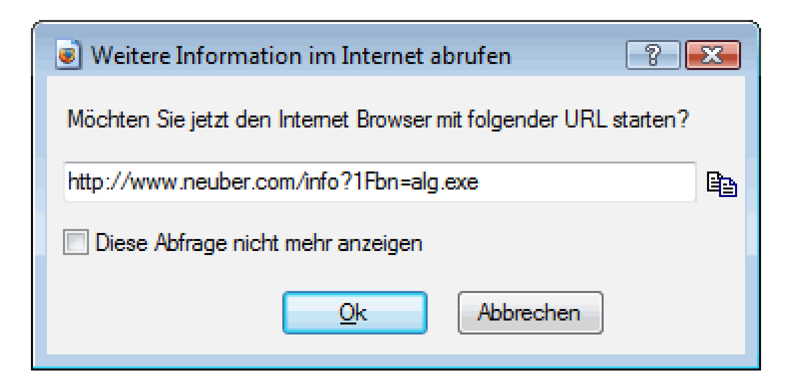
- Klicken Sie auf den Button **Online Info** 24, um im Internet verfügbare Informationen und Meinungen zu diesem Prozess zu sehen.
- Per Doppelklick auf einen Prozess sehen Sie eine Übersicht aller Daten des Prozesses.
- Klicken Sie auf **Konfiguration**, um als sicher eingestufte Prozesse auszublenden. Dies erhöht die Übersicht. Als sicher gelten z.B. digital signierte Betriebssystem-Prozesse.

Anzeigen von weiteren Eigenschaften (Google Suche)

Zu jedem Prozess können Sie sich eine Informationsseite angezeigen lassen, auf der Sie Ihren Kommentar zu dieser Software/Treiber abgeben können oder Kommentare anderer Administratoren lesen können. Von dieser Seite aus können Sie bei Google.com nach weiteren Informationen über diesen Prozess suchen.

1. Klicken Sie auf den Prozess, über welchen Sie mehr erfahren möchten.
2. Klicken Sie auf den Button **Online Info**.

Nach Klick auf den Button **Online Info** sehen Sie die zu öffnende URL. Klicken Sie auf **OK**, um Ihren Browser mit der angezeigten URL zu starten.



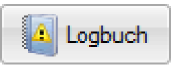
Die URL enthält den Dateinamen bzw. Fehlercode sowie die CRC Prüfsumme inklusive der Programmversion.

Anmerkung

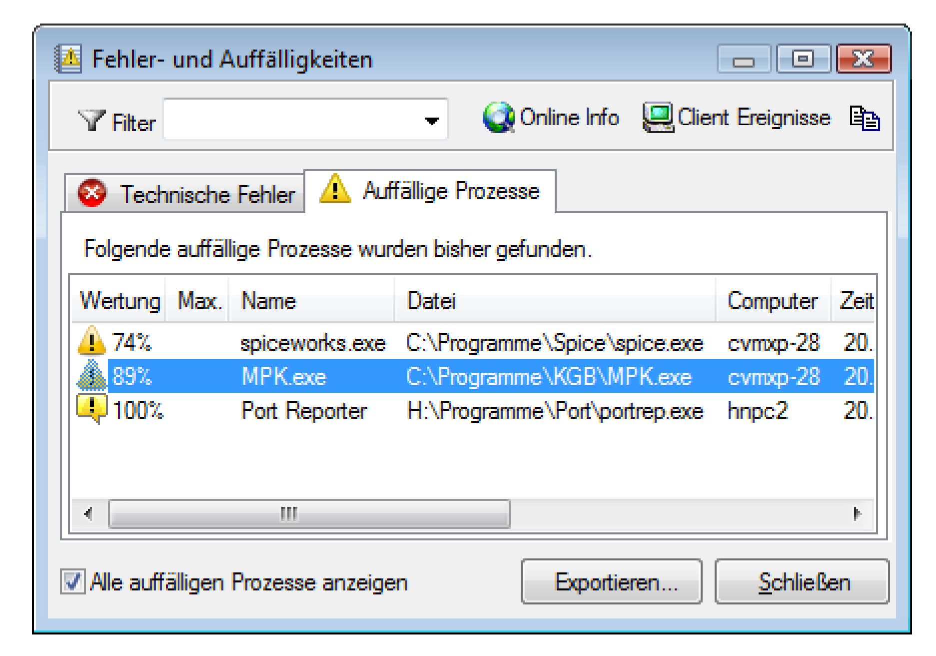
- Wenn Sie als Administrator in Windows angemeldet sind, wird die Benutzung des Browser nicht empfohlen. In diesem Fall kopieren Sie bitte die URL und gehen auf einem anderen PC mit weniger Rechten online.
- Aktivieren Sie die Option **Diese Abfrage nicht mehr anzeigen**, um den Browser direkt zu starten. Sie machen obigen Dialog wieder sichtbar, indem Sie die Strg-Taste drücken während Sie auf den Button **Online Info** klicken.

Ansehen des Auffälligkeiten-Protokolls

Eine Zusammenfassung über alle in der Vergangenheit erkannten potenziell gefährlichen Prozesse finden Sie im Logbuch.

1. Klicken Sie in der Programm Symbolleiste auf  

2. Klicken Sie auf die Registerkarte **Auffällige Prozesse**.
3. Sie sehen nun alle potenziell gefährlichen Prozesse, welche bei älteren Scans erkannt wurden.



Die Spalte **Wertung** zeigt die Risiko-Bewertung 28 beim letzten Auftreten des Prozesses. Die Spalte **Max** zeigt die höchste Bewertung seit dessen ersten Auftreten.

Der Prozess wurde bei einem Komplettscan des Computers erkannt.

Der Agent auf dem Computer hat den Admin per Popup Fenster auf dem Admin-PC 17 informiert. Ein Komplettscan fand nicht statt.

Filter bestimmt einen Computer, dessen Prozesse angezeigt werden.

Online Info zeigt Online detailierte Informationen und Meinungen zu dem markierten Prozess.

Stoppen eines Prozesses

1. Klicken Sie auf den Prozess, welchen Sie beenden möchten.
2. Klicken Sie im Menü **Bearbeiten** auf **Entfernen**.
3. Wählen Sie nun eine der folgenden Optionen:

Prozess beenden
Der Prozess wird aus dem Arbeitsspeicher entfernt. Sollte der Prozess in der Registry (Windows-Konfigurationsdatenbank) als Autostart eingetragen sein, so ist er jedoch beim nächsten Windows-Start wieder aktiv.

Datei in Quarantäne verschieben
Auch hier wird der Prozess aus dem Arbeitsspeicher entfernt. Zusätzlich wird die entsprechende Datei in den Quarantäne-Ordner26 (Menü Bearbeiten|Quarantäne...) verschoben und Autostart-Einträge in der Registry gelöscht. Da Datei und Registry-Einträge gesichert werden, ist eine Wiederherstellung des Prozesses möglich.

Anmerkung

- Das Beenden eines Prozesses kann zu Instabilitäten und Datenverlust führen. Programme oder auch Windows können abstürzen. Wir empfehlen deshalb, einen Prozess testhalber erst zu beenden. Wenn hierbei der Computer stabil weiterläuft, kann der Prozess nach dem nächsten Neustart in Quarantäne verschoben werden.

Quarantäne-Ordner

Der Quarantäne-Ordner funktioniert wie ein Papierkorb für beendete Prozesse. Wenn Sie eine Datei in den Quarantäne-Ordner verschieben26, so wird die Datei in einen abgeschotteten Ordner verschoben und umbenannt. Auch Autostart-Einträge dieses Prozesses in der Registry werden gelöscht. Damit ist die Datei nicht mehr ausführbar. Da Network Security Taskmanager alle seine Aktivitäten speichert, ist eine Wiederherstellung des Prozesses möglich.

So stellen Sie Prozesse wieder her

1. Klicken Sie im Menü **Bearbeiten** auf **Quarantäne Ordner...**

2. Klicken Sie im Quarantäne-Ordner auf den gewünschten Prozess.

3. Klicken Sie auf den Button **Wiederherstellen**.

Manuelle Wiederherstellung

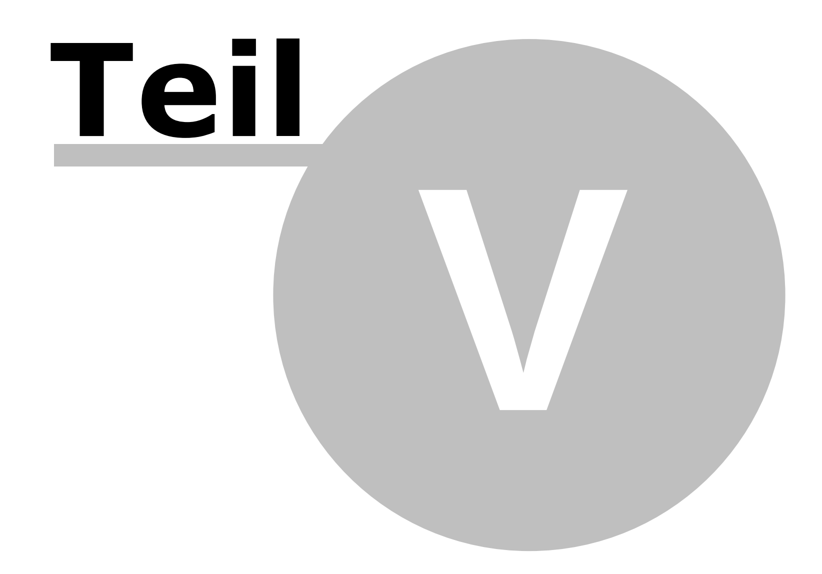
Die in Quarantäne verschobenen Dateien werden in folgendem Ordner gesichert:

- **`C:\ProgramData\Network Security Task Manager`** (unter Windows 8/7/Vista)
- **`C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Network Security Task Manager`** (unter Windows XP)

Die Dateien werden zur Sicherheit umbenannt in *dateiname.exe.irgendwelcheZahlen*, z.B. *optimizer.exe.q_1182E08_q*

Weiterhin werden die Dateien verschlüsselt. Im Notfall können Sie uns42 die Dateien zur Entschlüsselung schicken.

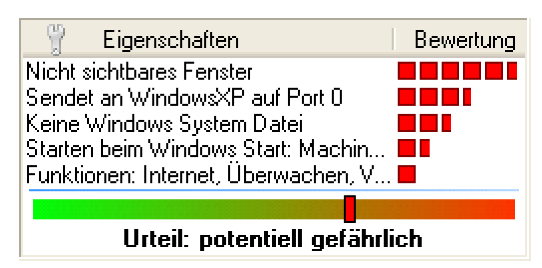
Grundlagen



V. Grundlagen

Risiko-Bewertung der Prozesse

Network Security Taskmanager bewertet das sicherheitsrelevante Risiko eines Prozesses nach objektiven Kriterien. Hierzu wird untersucht, ob der Prozess kritische Funktionsaufrufe oder verdächtige Eigenschaften enthält. Je nach potenzieller Gefährlichkeit dieser Funktionen und Eigenschaften werden Punkte vergeben. Die Summe ergibt dann die Gesamtwertung (0 bis maximal 100 Punkte).



Network Security Taskmanager untersucht die Prozesse nach folgenden Funktionalitäten (Sortierung nach Gefährlichkeit):

- **Kann Tastatur-Eingaben aufzeichnen**
  Der Prozess überwacht jede Tastatureingabe. Per Hook werden die Eingaben mitgelesen. Sauber programmierte, seriöse Programme nutzen diese Hook-Funktion nicht.
- **Getarnter Prozess ist unsichtbar**
  Der Prozess tarnt sich durch Windows API Hooking. Interne Windows Systembefehle zum Auflisten von Prozessen werden manipuliert. Dieser Prozess ist deshalb im Windows Task-Manager oder mit anderen Prozess-Viewern nicht zu finden. Wir empfehlen, diesen Prozess unter Quarantäne zu stellen. Hierzu klicken Sie im Menü **Bearbeiten** auf **Entfernen**.
- **Datei ist nicht sichtbar**
  Die Datei versteckt sich vor dem Windows Explorer. Die Datei ist mit einem Dateimanager nicht zu sehen. Diese Tarnfunktion ist nicht identisch mit dem harmlosen Dateiattribut "versteckt".
- **Tastatur-Treiber, könnte Eingaben aufzeichnen**
  Es handelt sich um einen Tastatur-Treiber, der jede Eingabe mitlesen kann.
- **Kann andere Programme manipulieren**
  Der Prozess kann sich in andere Programme einklinken und dort etwas verändern. Hierzu wird ein Hook gesetzt, der z.B. allen Programmen eine gefälschte Dateiliste vortäuschen kann (dir-Befehl ändern). Das Programm ist dann für andere Programme (AntiVirus) unsichtbar.
- **Kann Internet Browser überwachen**
  Browser Helper Objects (Browser PlugIns) klinken sich in den InternetExplorer ein. Meistens handelt es sich um erwünschte Download-Manager oder andere kleine Tools. Allerdings können BHO's auch Ihr Surfverhalten überwachen. Einzelne BHO's deaktivieren Sie im InternetExplorer Menü **Extras** unter **Add-Ons verwalten**.
  Um BHO's generell abzuschalten, klicken Sie im Internet Explorer im Menü **Extras** auf **Internetoptionen** und deaktivieren im Reiter **Erweitert** die Option **Browsererweiterungen von Drittanbietern aktivieren**.
- **Startet beim Start anderer Programme**
  Die Datei wurde über den Befehl ShellExecute in der Windows Systemregistrierung (Konfigurationsdatei) per Hook gestartet. ShellExecute startet einen Prozess (meistens eine DLL) sobald ein beliebiges Windows Programm gestartet wurde. Dieser Prozess sollte genau untersucht werden.
- **Lauscht auf Port <Nr>**
  Der Prozess kann über diese offene Stelle Informationen empfangen. Hacker nutzen solche Schwachstellen aus, um in einen fremden Rechner einzudringen und die Kontrolle über diesen zu erlangen. Mit einer guten Firewall können solche Attacken verhindert werden.
- **Sendet an <Computername> auf Port <Nr>**
  Der Prozess hat eine Verbindung zum angegebenen Computer bzw. zur IP-Adresse hergestellt und kann darüber beliebige Informationen senden. Mit einer guten Firewall können solche Verbindungen geblockt werden.
- **Unbekanntes Programm lauscht oder sendet**
  Es wurde ein Port geöffnet, um Informationen von außen zu empfangen oder dorthin zu senden. Bitte stellen Sie fest, um welches Programm es sich handelt. Mit einer guten Firewall kann die Verbindung blockiert werden.

- **Überwachen von Programmstarts**
  Der Prozess zeichnet auf, wann welche Programme aufgerufen und beendet werden.
- **Nicht sichtbares Fenster**
  Das Programm hat kein sichtbares Windows Fenster und läuft im Hintergrund. Im günstigsten Fall handelt es sich z.B. um Gerätetreiber.
- **Starten beim Windows Start**
  Das Programm wird bei jedem Windows-Start aufgerufen. Hierzu hat sich das Programm in einem Autostart-Schlüssel in der Windows Systemregistrierung eingetragen.
- **Keine ausführliche Beschreibung vorhanden**
  Einige wichtige Standard-Beschreibungen in der Datei sind nicht vorhanden. Standardmäßig enthält jede Datei interne Felder für Beschreibungen.
- **Unbekannte Datei im Windows Ordner**
  Die Datei gehört nicht zum Windows Betriebssystem. Sie wurde in das Windows-Verzeichnis kopiert. Dies kann an einer schlecht programmierten Software liegen oder die Datei versucht sich im Windows-Verzeichnis zu verstecken.
  Vorsicht ist geboten, wenn Sie diese Datei keinem installierten Software-Produkt oder Hardware-Treiber zuordnen können.
- **Keine Windows System Datei**
  Die Datei gehört nicht zum Windows Betriebssystem. Erhöhte Aufmerksamkeit ist erforderlich, wenn sich die Datei im Windows Verzeichnis befindet und sich diese Datei keinem installierten Software-Produkt oder Hardware-Treiber zuordnen lässt.
- **Fehlende Beschreibung des Programms**
  Es sind keine Beschreibungen in der Datei vorhanden. Standardmäßig enthält jede Datei intern einige Felder für Beschreibungen.
- **Funktionen: Internet, Überwachen, Eingabe aufzeichnen, Verstecken, Manipulieren**
  Die Datei enthält Funktionsaufrufe mit den angegebenen Eigenschaften. Da jedoch nicht gesagt werden kann, ob und wie diese zum Einsatz kommen, wichtet der Network Security Task Manager dieses Kriterium nicht stark.
- **Funktionen: nicht ermittelbar**
  In der Datei wurden keine gefährlichen Funktionsaufrufe gefunden. Diese könnten jedoch versteckt integriert sein.
- **Unbekannter Hersteller**
  Der Hersteller ist nicht ermittelbar. Standardmäßig enthält jede Datei intern Felder zur Angabe des Softwareherstellers.

Vertrauenswürdige Eigenschaften (verbessern die Risiko-Bewertung):

- **Microsoft signierte Datei**
  Diese Datei wurde von Microsoft signiert. Sie können dieser Datei vertrauen, so wie Sie auch Microsoft vertrauen.
- **Verisign signierte Datei**
  Diese Datei wurde von VeriSign signiert. Sie können dieser Datei vertrauen, so wie Sie auch VeriSign vertrauen.
- **Gehört zu <Software Produkt> von <Hersteller>**
  Diese Datei ist als vertrauenswürdig eingestuft. Sie gehört zu der genannten, installierten Software. Wenn Sie die Software in der Systemsteuerung deinstallieren, so löschen Sie auch diese Datei.
- **Zertifiziert von <Hersteller>**
  Diese Datei wurde von einer Zertifizierungsstelle signiert. Sie können dieser Datei vertrauen, so wie Sie auch der Zertifizierungsstelle und dem Softwarehersteller vertrauen.
- **Eigener Kommentar**
  In der Referenzdatenbank speichern Sie die Prozesse, die Ihnen bekannt sind. Jeden Prozess können Sie kommentieren und als ungefährlich einstufen.

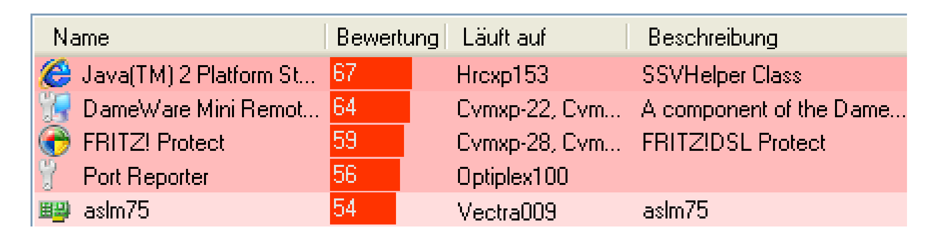
Weitere Informationen 19

Anmerkung

- Hoch bewertete Prozesse müssen nicht zwingend gefährlich sein. Sie besitzen eventuell nur für Malware typische Funktionen.
  Beispiel: Systemüberwachung durch Antivirus-Wächter/Firewall.
- Klicken Sie auf **Konfiguration**, um als sicher eingestufte Prozesse auszublenden. Das Ausblenden von Windows-Systemprozessen erhöht die Übersicht.

Prozess-Typen

Network Security Taskmanager unterscheidet verschiedene Arten von Prozessen:



Name	Bewertung	Läuft auf	Beschreibung
Java(TM) 2 Platform St...	67	Hrcxp153	SSVHelper Class
DameWare Mini Remot...	64	Cvmxp-22, Cvm...	A component of the Dame...
FRITZ! Protect	59	Cvmxp-28, Cvm...	FRITZ!DSL Protect
Port Reporter	56	Optiplex100	
aslm75	54	Vectra009	aslm75

Im Menü **Ansicht** können Sie unter **Spalten auswählen** einstellen, dass auch der **Typ** in einer Tabellenspalte angezeigt wird. Sie können jedoch auch am Icon erkennen, um welchen Typ es sich handelt:

Prozess mit Fenster
Ein normales Programm mit sichtbarem Windows Fenster.
Beispiel: Word

Prozess ohne Fenster
Ein Programm, dass im Hintergrund läuft. Das Programm hat kein Fenster oder es befindet sich im nicht sichtbaren Bereich.
Beispiel: Backup Prozess, Virus-Wächter; aber auch Trojaner

Prozess mit einem Icon in der Taskleiste
Ein Programm, dessen Icon in der Taskleiste (links neben der Uhrzeit) verankert ist. Klicken Sie mit der rechten Maustaste auf das Icon in der Taskleiste, um ein Kontextmenü zu öffnen und mehr über das Programm zu erfahren.
Beispiel: Firewall, NetTaskTray 31

Internet Explorer PlugIn
Browser Helper Objects klinken sich in den InternetExplorer ein. Meistens handelt es sich um erwünschte Download-Manager oder andere kleine Tools. Allerdings können BHO's auch Ihr Surfverhalten überwachen.
Einzelne BHO's deaktivieren Sie im Internet Explorer Menü **Extras** unter **Add-Ons verwalten.**
Um BHO's generell abzuschalten, klicken Sie im Internet Explorer im Menü **Extras** auf **Internetoptionen** und deaktivieren im Reiter **Erweitert** die Option **Browsererweiterungen von Drittanbietern aktivieren.**
Beispiel: Adobe PDF Reader, Java Konsole; aber auch Spyware

DLL Datei
Eine Dynamic Link Library (DLL) enthält ausführbaren Programmcode. In einer DLL-Datei sind im Standardfall selten genutzte Funktionen ausgelagert, die nur bei Bedarf vom Hauptprogramm ausgeführt werden. Dadurch benötigt das Hauptprogramm weniger Arbeitsspeicher.

DLL Datei (per ShellExecute)
Die Datei wird über den Befehl ShellExecute in der Windows Systemregistrierung (Konfigurationsdatei) per Hook gestartet. ShellExecute startet einen Prozess (meistens eine DLL), sobald ein beliebiges Windows-Programm gestartet wurde. Dieser Prozess sollte genau untersucht werden.

Windows Systemprozess (signiert)
Ein von Microsoft digital signierter Prozess, der zum Windows Betriebssystem gehört. Fast alle Betriebssystemprozesse sind digital signiert.
Beispiel: explorer.exe, winlogon.exe

Windows Systemprozess
Prozess, der zum Windows Betriebssystem gehört.
Beispiel: system idle

Treiber und Dienste

Gerätetreiber
Gerätetreiber zum Betrieb von Hardwarekomponenten. Das können Treiber für Grafikkarte und Scanner sein. Aber auch Programme, die nicht von einem Benutzer oder Programm beendet werden sollen (z.B. Firewall, AntiVirus-Modul).

Dateitreiber
Treiber für das auf Windows NT basierende Dateisystem.

Dienst (eigener Prozess)
Ein system- oder hardwarenaher Prozess zur Unterstützung anderer Programme. Der Dienst wird als eigener Prozess ausgeführt.

Dienst (eigener Prozess mit Desktop-Interaktion)
Ein system- oder hardwarenaher Prozess zur Unterstützung anderer Programme. Der Dienst wird als eigener Prozess ausgeführt, der mit dem Desktop interagieren kann (z.B. Firewall, AntiVirus-Modul).

Dienst (beteiligter Prozess)
Der Dienst teilt sich mit anderen Diensten einen Prozess.

Dienst (beteiligter Prozess mit Desktop-Interaktion)
Der Dienst teilt sich mit anderen Diensten einen Prozess. Der Prozess kann mit dem Desktop interagieren.

Anmerkung

- Um die Übersicht zu erhöhen, können Sie alle Windows-Systemprozesse ausblenden 18.

Was ist NetTaskTray

NetTaskTray nennt sich das Tool, welches Sie nach dem Start von Network Security Taskmanager 5 in der Taskleiste neben der Uhr sehen.



NetTaskTray ist verantwortlich für:

Zeitplanung
NetTaskTray stößt die zeitgesteuerte Prozess-Prüfung auf den Arbeitsplatzrechnern an. Die Zentralkomponente muss also nicht laufen, um Computer regelmäßig und automatisch zu scannen.

NetTaskTray muss in einem Benutzerkonto laufen, das Administrator-Rechte auf dem zu scannenden Computer hat.

Warnung des Administrators bei Auffälligkeiten
NetTaskTray zeigt ein kleines Popup, wenn ein Arbeitsplatzrechner einen potenziell gefährlichen Prozess meldet. Der Arbeitsplatzrechner kontaktiert also nicht direkt die Zentralkomponente. NetTaskTray nimmt die Warnmeldung entgegen, prüft die Meldung und leitet sie an die Zentralkomponente weiter.

Damit NetTaskTray die Meldungen von den Arbeitsplatzrechnern (mit Zeitplanung *Beim Start eines Prozesses* oder *Nach dem Booten des Client*) empfangen kann, muss auf dem Computer, auf dem die Zentralkomponente läuft, die Datei- und Druckerfreigabe 7 aktiviert sein.

Anmerkung

- Erkennt der Agent-Dienst auf dem Arbeitsplatzrechner einen potenziell gefährlichen Prozess, so wird der Administrator auf verschiedenen Wegen gewarnt 17. Somit ist sichergestellt, dass die Warnung auch bei Netzwerk-Problemen nicht verloren geht.

Admin$ Freigabe

Eine versteckte Freigabe ist durch ein Dollarzeichen ($) am Ende des Freigabenamens gekennzeichnet. Versteckte Freigaben werden nicht aufgelistet, wenn Sie die Freigaben auf einem Computer durchsuchen oder den Befehl **net view** verwenden.

Der System Ordner c:\windows (Variable %SYSTEMROOT%) wird als ADMIN$ freigegeben. Diese administrative Freigabe erlaubt dem Administrator den Fernzugriff auf den lokalen Windows Ordner der Computer im Netzwerk.

Um einen Windows 8/7/Vista Computer in einer **Arbeitsgruppe** zu scannen, sind folgende zusätzliche Einstellungen 34 nötig.

So überprüfen Sie, ob *Admin$* auf dem Arbeitsplatzrechner verfügbar ist

- Auf dem Arbeitsplatzrechner führen Sie in der Eingabeaufforderung (Start > Alle Programme > Zubehör > Eingabeaufforderung) den Befehl **net share** aus. Dort sollte Admin$ als Freigabe angezeigt werden.
- Von einem beliebigen Computer im Netzwerk geben Sie im Windows Explorer als Adresse ein: **\\zielrechner\admin$**
  Alternativ in der Eingabeaufforderung (z.B. **cmd** ausführen) **dir \\zielrechner\admin$**
  Sie sehen nun den Windows Ordner des Arbeitsplatzrechners.
- Folgende Programme zeigen Ihnen alle im Netzwerk verfügbaren Adminfreigaben an:
  Microsoft Baseline Security Analyzer (kostenlos)
  GFI LAN guard - Network Security Scanner (kostenpflichtig)
  Hyena (kostenpflichtig)

Erstellen der administrativen Freigabe Admin$

Gehen Sie folgendermaßen vor, falls die Freigabe Admin$ auf einem Computer nicht verfügbar ist:

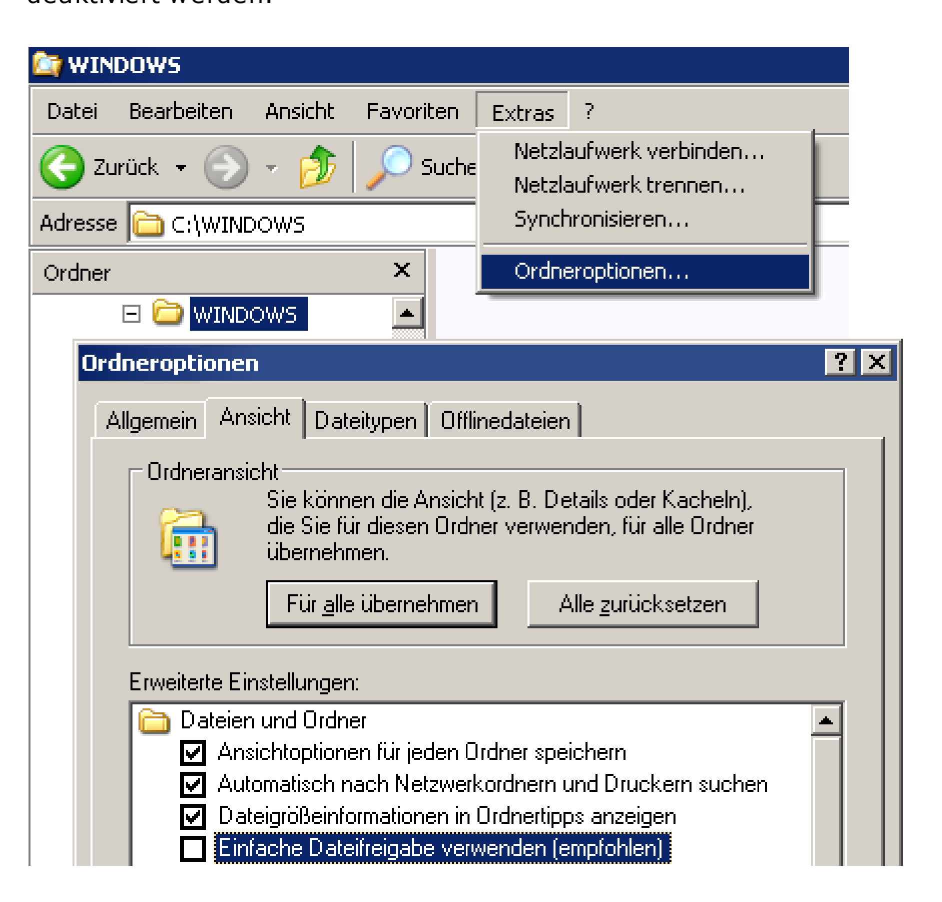
1. Doppelklicken Sie in der Systemsteuerung auf **Verwaltung** und dann auf **Computerverwaltung**.
2. Erweitern Sie **Freigegebene Ordner**, klicken Sie mit der rechten Maustaste auf **Freigaben,** und klicken Sie auf **Neue Dateifreigabe**.
3. Geben Sie im Feld **Freizugebender Ordner** den Pfad %SYSTEMROOT% ein.
4. Geben Sie ein: Admin$ und klicken Sie auf **Weiter**.
5. Aktivieren Sie das Kontrollkästchen **Administratoren haben Vollzugriff, andere Benutzer haben keinen Zugriff**, um den Zugriff auf die Freigabe nur Administratoren zu gewähren.
6. Klicken Sie auf **Fertig stellen**.
7. Klicken Sie auf **Nein**, um zur Computerverwaltungskonsole zurückzugehen.

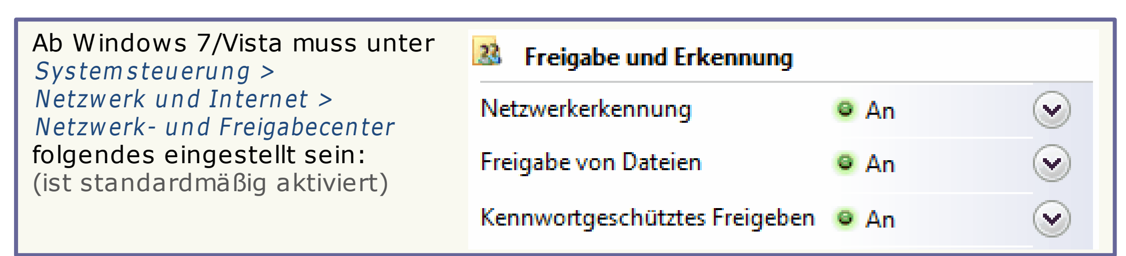
Alternativ können Sie auf dem lokalen Computer in der Eingabeaufforderung (cmd ausführen) den Befehl **net share admin$** ausführen.

Einfache Dateifreigabe

Falls *Network Security Taskmanager* einen Computer in der **Arbeitsgruppe** nicht scannen kann, so deaktivieren Sie bitte die "Einfache Dateifreigabe" auf diesem Arbeitsgruppen-Computer. Falls auf diesem Arbeitsgruppen-Computer Windows 8/7/Vista läuft, so beachten Sie bitte folgende Hinweise 34.

Die **einfache Dateifreigabe** wird unter Windows XP im Windows Explorer im Menü **Extras** in den **Ordneroptionen** deaktiviert. Je nach Einstellung wirkt sich dies aber nur auf den aktuellen Ordner aus. Daher muss noch die Option "Ansichtsoptionen für jeden Ordner speichern" deaktiviert werden.





Damit ist nun im Eigenschaftsdialog von Ordnern und Dateien die Registerkarte **Sicherheit** eingeblendet.
Folgender Registry Schlüssel ist für die "Einfache Dateifreigabe" zuständig:
`HKEY_LOCAL_MACHINE\ System\CurrentControlSet\Control\LSA`

forceguest = **0** - "Einfache Dateifreigabe" nicht verwenden
forceguest = **1** - "Einfache Dateifreigabe" verwenden (Standard)

Der Eintrag kann auch über die lokalen Sicherheitsrichtlinien (Verwaltung -> lokale Sicherheitsrichtlinien -> lokale Richtlinien -> Sicherheitsoptionen -> Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten) editiert werden.

Die "Einfache Dateifreigabe" wird unter Windows XP Professional standardmäßig dann aktiviert, wenn bei der Installation des Betriebssystems der Computer zu einer Arbeitsgruppe hinzugefügt wird. Wird bei der Betriebssysteminstallation der Computer direkt zu einer Domäne hinzugefügt, dann ist die "Einfache Dateifreigabe" standardmäßig deaktiviert.

Wird ein in einer Arbeitsgruppe befindlicher Computer nachträglich in eine Domäne gehoben, bleibt die Einstellung "Einfache Dateifreigabe verwenden" trotzdem bestehen und muss, wenn unerwünscht, wie oben beschrieben abgeschaltet werden.

Windows 8/7/Vista Zielrechner

Bitte beachten Sie folgende Hinweise, wenn Sie einen Computer scannen möchten, auf dem **Windows 8/7/Vista** läuft und der sich **in einer Arbeitsgruppe** befindet.

> Gehört der zu scannende Computer keiner Arbeitsgruppe an, sondern einer **Domäne**, so sind die folgenden Hinweise nicht zu beachten, weil ein Domänenadministrator stets Zugriff auf die administrative Freigabe admin$ eines Computers in der Domäne hat.

Standardmäßig verhindert die Benutzerkontensteuerung (UAC) von Windows 8/7/Vista, dass man über das Netzwerk auf die administrative Freigabe admin$ eines Arbeitsgruppen-Computers zugreifen kann. *Network Security Taskmanager* zeigt deshalb bei dem Versuch, einen Windows 8/7/Vista Arbeitsgruppen-Computer zu scannen, die Fehlermeldung: **Benutzer <Benutzername> hat keine Administrator-Rechte auf <Clientcomputer>**

Lösung:
Microsoft empfiehlt folgende Lösung (KB947232) um auf die administrative Freigabe admin$ bei Windows 8/7/Vista Computern in einer Arbeitsgruppe mit einem lokalen Administratorkonto zugreifen zu können. Hierbei bleibt die Sicherheit des übrigen Benutzerkontenschutzes (UAC) bestehen. Damit kann *Network Security Taskmanager* diesen Windows 8/7/Vista Arbeitsgruppen-Computer remote scannen:

1. Auf dem Windows 8/7/Vista Zielrechner starten Sie den Registrierungs-Editor (regedit.exe).
2. Gehen Sie zu folgendem Schlüssel:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. Klicken Sie im Menü **Bearbeiten** auf **Neu**, und dann auf **DWORD-Wert (32-Bit)**.
4. Geben Sie **LocalAccountTokenFilterPolicy** als Namen für den neuen Eintrag ein.
5. Klicken Sie mit der rechten Maustaste auf LocalAccountTokenFilterPolicy, und dann auf **Ändern**.
6. Geben Sie in das Feld **Wert** den Wert **1** ein. Klicken Sie nun auf **OK** und beenden Sie den Registrierungs-Editor.

Anmerkung

- Alternativ können Sie den Agent auch dauerhaft auf dem Windows 8/7/Vista Arbeitsgruppen-Computer installieren. Hierzu starten Sie auf dem Windows 8/7/Vista Arbeitsgruppen-Computer die Datei **NetTaskAgent.msi** 50, welche sich im Programmordner (z.B. in c:\Programme\Network Security Taskmanager\) befindet. Dann sind obige Schritte 1- 6 nicht notwendig.

Absicherung der Microsoft Netzwerkkommunikation

Die Microsoft Netzwerkkommunikation (SMB, NetBIOS) kann je nach Aufbau des Windows-Netzwerks weiter abgesichert werden.

NTLMv2, 128-Bitverschlüsselung

Die weiteren Microsoft Netzwerkkommunikations-Absicherungsmaßnahmen können über die Gruppenrichtlinie aktiviert werden:

1. Öffnen Sie die Eingabeaufforderung (Start > Alle Programme > Zubehör > Eingabeaufforderung) als Administrator.
   Alternativ: Start > Ausführen: "runas /user:Administrator cmd" eingeben und ausführen. Dann das Administrator-Passwort eingeben
2. Im neu geöffneten DOS-Fenster nun "gpedit.msc" eingeben und die <Enter>-Taste drücken.
3. Im linken Fensterteil zu den Sicherheitsoptionen wechseln:Computerkonfiguration -> Windows-Einstellungen -> Lokale Richtlinien -> Sicherheitsoptionen

Entnehmen Sie bitte dem IT-Grundschutzhandbuch Kapitel M 5.123 "Absicherung der Netzwerkkommunikation unter Windows XP": http://www.bsi.de/gshb/deutsch/m/m05123.htm

welche Absicherungsmaßnahmen für Ihre Windows-Netzwerktopologie in Frage kommen. Beachten Sie unbedingt die Hinweise von Microsoft: http://support.microsoft.com/kb/823659

wann und wo eine weitere Absicherungsmaßnahme zu Problemen führen könnte! Es wird dringend empfohlen, in Windows-Netzwerken ausschließlich das Authentifizierungsverfahren NTLMv2 zu verwenden. Siehe auch: Knacken von Windows-Passwörtern in Sekunden

NetBIOS über TCP/IP (NetBT)

Die Einstellung *NetBIOS über TCP/IP* kann bei Netzwerken mit einer über den DNS-Server laufenden Namensauflösung deaktiviert werden, falls sich kein einziger Windows 9x/ME oder Windows NT-Rechner im Netzwerk befindet:

1. Startmenü -> Systemsteuerung -> Netzwerkverbindungen
2. Doppenklicken Sie die gewünschte Netzwerkverbindung.
3. Klicken Sie nun im Kontexmenü auf **Eigenschaften**.
4. Doppelklicken Sie **Internetprotokoll TCP/IP**.
5. Klicken Sie auf den Button **Erweitert**.
6. Klicken Sie die Registerkarte **WINS**.
7. Wählen Sie die Option **NetBIOS über TCP/IP deaktivieren**.
8. Schließen Sie nun alle Netzwerkverbindungsfenster.

Bei ausgeschaltetem NetBIOS über TCP/IP erfolgen die Zugriffe auf die Netzwerkfreigaben (SMB-Kommunikation) direkt über den TCP-Port 445.

NetBIOS über TCP/IP mit der Firewall blocken

Die UDP-Ports 137, 138 und der TCP-Port 139 werden mit der Abschaltung von NetBIOS über TCP/IP frei. Der Zugriff von außen auf die drei nicht mehr genutzten Ports sollte per Firewall verhindert werden:

1. Startmenü -> Systemsteuerung -> Windows Firewall
2. Klicken Sie die Registerkarte **Ausnahmen**.
3. Doppenklicken Sie **Datei- und Druckerfreigabe**.
4. Setzen Sie einen Haken bei **TCP 445**. Bei allen anderen Ports den Haken entfernen.
5. Alle offenen Windows Firewall-Fenster schließen.

Verwendete Dateien und Prozesse

Network Security Taskmanager benötigt auf dem Administrator Computer und auf den zu scannenden Computern nur eine Windows Standardinstallation 7. Zusätzliche Treiber, Libraries und Dienste werden nicht benötigt.

Werden bestehende Systemdateien, Libraries, Treiber etc. bei der Installation geändert?

Nein. Die Installation von Network Security Taskmanager auf einem Computer ändert weder Registry noch vorhandene Dateien. Es werden keine Dateien außerhalb des angegebenen Installationverzeichnisses erstellt oder verändert.

Wird Network Security Taskmanager gestartet, so speichert die Software ihre Daten hier ab:

- In der Registry im Schlüssel **HKEY_CURRENT_USER\Software\Neuber\Network Security Task Manager**
- auf der Festplatte im Ordner **C:\ProgramData\Network Security Task Manager** (unter Windows 8/7/Vista) **C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Network Security Task Manager** (unter Windows XP)

Der Registry Schlüssel und der angelegte Ordner werden bei einer Programm Deinstallation 38 wieder gelöscht.

Welche Prozesse sind auf dem Administrator Computer aktiv?

Auf dem Computer, wo der Administrator mit Network Security Taskmanager arbeitet, laufen folgende Prozesse:

NetTaskConsole.exe - die Admin Console 5, d.h. das Hauptprogramm

NetTaskTray.exe 31 - steuert Zeitplanung und Warnungseingang im Tray der Taskleiste

Welche Prozesse sind auf einem Arbeitsplatz-Rechner aktiv?

Auf dem gescannten Clientcomputer wird während des Scans die Datei **NetTaskAgent.exe** in die lokale Admin-Freigabe Admin$ 32 kopiert und als Dienst gestartet. Nach dem Scan wird dieser Agent-Dienst wieder vollständig entfernt.

Nur auf Computern mit der Zeitplanung *Beim Start eines Prozesses* oder *Nach dem Booten des Clients* wird der Agent-Dienst dauerhaft installiert.

Der Agent-Dienst speichert Cache Daten auf dem gescannten Clientcomputer in folgenden Ordnern:

- **C:\ProgramData\Network Security Task Manager** (unter Windows 8/7/Vista)
- **C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Network Security Task Manager** (unter Windows XP)

Diese Ordner wird stets gelöscht, wenn der Clientcomputer aus der Console entfernt 14 wird.

Anmerkung

- Hinweis: Aus Sicherheitsgründen wird die Agent-Datei NetTaskAgent.exe auf den Clients unter einem zufälligen Namen gespeichert, z.B. als smPolodo.exe. Mit mit dem Befehl **sc \\zielcomputer qc nettaskagent** erfahren Sie den wahren Dateinamen.

Rechtliche Aspekte

Network Security Taskmanager dient nicht zur Überwachung von Mitarbeitern. Es ist nicht möglich, das Verhalten von Mitarbeitern aufzuzeichnen.

Network Security Taskmanager wird im Rahmen der Netz- und Systemanalyse eingesetzt. Die Software erkennt Malware, welche von traditionellen signaturbasierten Sicherheitslösungen nicht erkannt wird. Network Security Taskmanager hilft somit Wirtschaftsspionage, Sabotage und sicherheitskritische Software aufzudecken.
Die Geschäftsleitung ist gesetzlich (KonTraG) verpflichtet, Systeme und Software einzurichten, "damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden". Wird dies unterlassen, können Vorstände oder Geschäftsführer persönlich haftbar gemacht werden.

Datenschutz

⊟ Keine personenbezogen Daten
Alle Daten werden computerbezogen gespeichert. Personenbezogene Daten werden nicht aufgezeichnet. Einzigste Ausnahme: Der beim letzten Scan eines Computers angemeldeten Benutzer wird protokolliert 13. Dies ist jedoch nach §14(2) BDSG zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erlaubt.
Die Aufzeichnung von Daten erfolgt nur in dem Umfang, wie es für die Erkennung von Angriffen, Angriffsversuchen und Sicherheitsverletzungen und deren Rückverfolgung erforderlich ist. Daten werden zu keinem anderen Zweck aufgezeichnet.
Die Aufzeichnung von Daten erfolgt also ausschließlich, um den ordnungsgemäßen Betrieb von Datenverarbeitungsanlagen sicherzustellen. Die von Network Security Taskmanager ermittelten Daten können auch mit Windows Boardmitteln von jedem Admin ermittelt werden.

⊟ Datenvermeidung und Datensparsamkeit
Es werden so wenig Daten wie möglich erhoben. Diese werden verschlüsselt gespeichert.

Wie bei anderer Sicherheitssoftware auch, sollte der Betriebs- oder Personalrat informiert werden.

⊟ Maßnahmen
- Datenschutzbeauftragte und Betriebs- bzw. Personalrat informieren
- Einsatz der Software in Dienst- oder Betriebsvereinbarung aufnehmen
- Mitarbeiter über Einsatz und Einsatzzweck informieren
  (Abhängig von der Einsatzweise bleibt zu prüfen, ob es erforderlich ist, dass betreffende Mitarbeiter ihr Einverständnis zum Einsatz erklären)
- Sämtliche Mitarbeiter, die die Software administrieren oder Zugriff auf deren Daten haben, sind auf das Datenschutzgesetz zu verpflichten.

Bundesdatenschutzgesetz
§14 (4) und §31: „Personenbezogene Daten, die ausschließlich [...] zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage genutzt werden, dürfen nur für diesen Zweck verwendet werden.“

§14 (2): „Das Speichern, Verändern oder Nutzen [...] ist [...] zulässig, wenn es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten [...] erforderlich ist.“

Weitere, allgemeine Informationen
http://www.it-sicherheitsrecht.info/9727.html
http://de.wikipedia.org/wiki/KonTraG
http://www.networkers.de/Juristische_Informationen.pdf
http://www.bsi.bund.de/literat/studien/ids02/evids_ra.htm

Deinstallieren der gesamten Software

So deinstallieren Sie den Agent-Dienst von Clientcomputern

Der Agent-Dienst wird dauerhaft auf dem zu scannenden Computer installiert bei
- Verteilung des Agent-Dienstes per MSI-Paket
- eingerichteter Zeitplanung *Beim Start eines Prozesses* oder *Nach dem Booten des Clients*

Sie haben folgende Möglichkeiten den Agent-Dienst von einem Computer zu entfernen:

Deinstallation im Network Security Taskmanager
Löschen Sie die Zeitplanung für die gewünschten Computer oder entfernen 14 Sie die Computer aus der Liste.

Deinstallation per Befehl
Als Administrator können Sie auch am Arbeitsplatzrechner mit dem Befehl **`NetTaskAgent.exe /u`** oder von einem entfernten Computer aus mit dem Befehl **`sc \\zielcomputer delete nettaskagent`** den Agent-Dienst komplett deinstallieren.

Deinstallation per Login Script
Sie können den Befehl **`NetTaskAgent.exe /u`** auch in einer Batch-Datei speichern und so den Agent-Dienst als **Loginscript** per Gruppenrichtline deinstallieren.
Im Unterschied zur msi-Anleitung 62 klicken Sie im Schritt *5* im Gruppenrichtlinienobjekt-Editor unter Computerkonfiguration > Windows-Einstellungen > Scripts (Start/Herunterfahren) auf "Starten". Klicken Sie dann auf "Hinzufügen", um die Batch Datei hinzuzufügen. Die Batch-Datei wird im lokalen Systemkonto - also mit Adminrechten - ausgeführt.

Deinstallation per Softwareverteilung / Gruppenrichtlinie
Haben Sie den Agent-Dienst per MSI-Paket auf die Computer verteilt, so können Sie den Agenten auch wieder mit Ihrer Softwareverteilungssoftware oder per Gruppenrichtline deinstallieren 66.

So deinstallieren Sie die Console 5

1. Öffnen Sie die Windows Systemsteuerung .
2. Klicken Sie auf **Software** (Programme deinstallieren).
3. Klicken Sie auf *Network Security Taskmanager*
4. Klicken Sie auf **Deinstallieren**.

Anmerkung

- Hinweis: Aus Sicherheitsgründen wird die Agent-Datei NetTaskAgent.exe auf den Clients unter einem zufälligen Dateinamen gespeichert, z.B. als smPolodo.exe. Mit mit dem Befehl **`sc \\zielcomputer qc nettaskagent`** erfahren Sie diesen richtigen Dateinamen.
  Für die Deinstallation des Agenten müssen Sie im Befehl diesen richtigen Dateinamen verwenden, z.B. **`smPolodo.exe /u`**

Troubleshooting



VI. Troubleshooting

Beheben von Verbindungsfehlern

Hinweis: Wenn Sie per Windows-Explorer wie folgt auf dem zu scannenden Computer zugreifen können, so funktioniert auch Network Security Taskmanager:

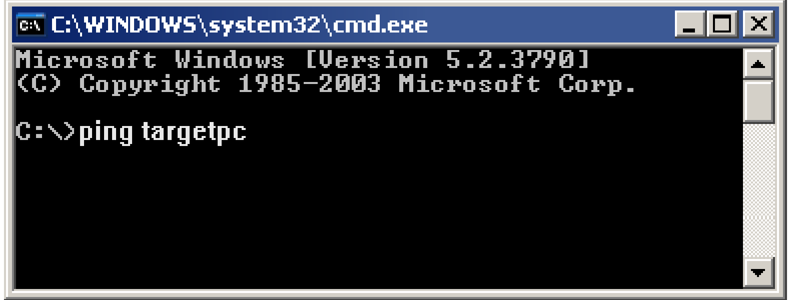


Was bei einem Windows 8/7/Vista Zielrechner zu beachten ist 34

Kann Network Security Taskmanager einen Computer nicht scannen, so überprüfen Sie, ob dort alle Voraussetzungen erfüllt sind:

Computer ist hochgefahren

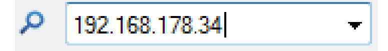
1. Überprüfen Sie, ob der zu scannende Computer im Netzwerk erreichbar ist. Hierzu geben Sie in der Eingabeaufforderung (Start > Alle Programme > Zubehör > Eingabeaufforderung) folgenden Befehl ein:
   ping *zielrechner*

   Ist der Computer nicht anpingbar, so überprüfen Sie, ob der Computer hochgefahren ist und der Computername korrekt geschrieben ist.

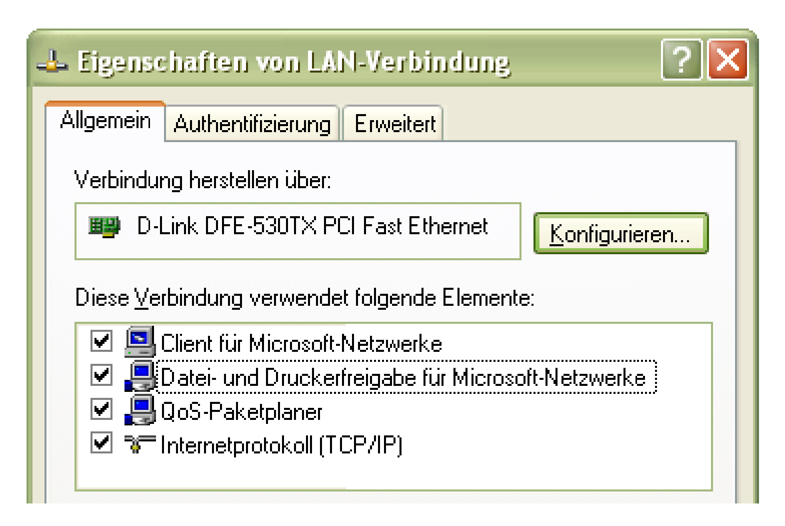
   Hinweis: Ein Computer ist nur anpingbar, wenn die Windows Firewall dies zulässt, unter: Erweitert > ICMP Einstellungen > Eingehende Echoanforderung zulassen (Default Einstellung). Network Security Taskmanager funktioniert unabhängig von dieser Einstellung.

2. Ist der Computer anpingbar, so notieren Sie die IP-Adresse des Zielrechners und verwenden diese in *Network Security Taskmanager* anstelle des Computernamens:

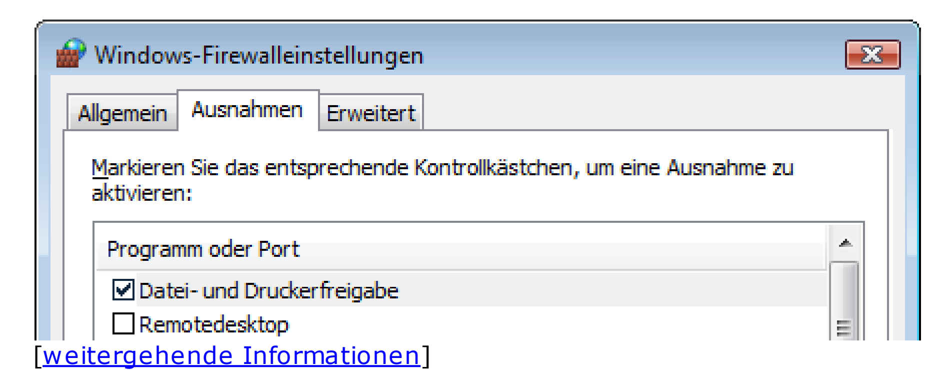
   

   Wenn der Scan nur mit der IP-Adresse funktioniert, so besteht zu dem Zielrechner entweder schon eine Verbindung unter einem anderen Benutzernamen 47 oder Namensauflösung für die Datei- und Druckerfreigabe 45 wird geblockt.

Datei und Druckerfreigabe
Aktivieren Sie auf dem zu scannenden Computer die "Datei- und Druckerfreigaben für Microsoft-Netzwerke" in der Systemsteuerung > Netzwerkverbindungen > rechter Mausklick auf die gewünschte LAN-Verbindung > Eigenschaften.



Firewall Ausnahme für Datei- und Druckerfreigabe
Die Firewall auf dem zu scannenden Computer darf die Datei-und Druckerfreigabe nicht blockieren. Das heißt der TCP-Port 445 (SMB Protokoll) muss offen sein.



[weitergehende Informationen]

Wenn in Ihrem Netzwerk **NetBIOS über TCP/IP** (NetBT) aktiv ist, so muss TCP-Port 139 (NetBIOS-Sitzungsdienst) für die Namensauflösung 44 offen sein.

Die "Datei und Druckerfreigabe" bitte nur an die Netzwerkkarte/Netzwerkverbindungen des internen Firmennetzwerkes binden! Die "Datei und Druckerfreigabe" darf nicht aktiviert sein bei Netzwerkverbindungen/Netzwerkkarten nach außen (zum Internet bzw. am Gateway).

Admin-Freigabe Admin$
Um einen Computer zu scannen, wird auf diesem kurzzeitig ein Agent-Dienst in den lokalen Windows Ordner (=Admin$) installiert.
Um zu überprüfen, ob auf dem zu scannenden Computer die Admin$ Freigabe existiert, führen Sie dort in der Eingabeaufforderung den Befehl **net share** aus. Es sollte Admin$ als Freigabe angezeigt werden.
Weitere Methoden zum Überprüfen der Admin$ Freigabe 32

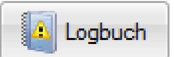
Gehört der zu scannende Computer keiner Domäne an, sondern einer Arbeitsgruppe, so deaktivieren Sie auf diesem die Einfache Dateifreigabe 33. Läuft dort Windows 8/7/Vista, so müssen Sie zusätzlich folgende Einstellung 34 vornehmen.

Wenn der Agent-Dienst per MSI-Paket 50 verteilt wurde oder eine Zeitplanung 15 *Beim Start eines Prozesses* oder *Nach dem Booten des Clients* schon besteht, so ist keine Adminfreigabe auf dem zu scannenden Computer erforderlich.

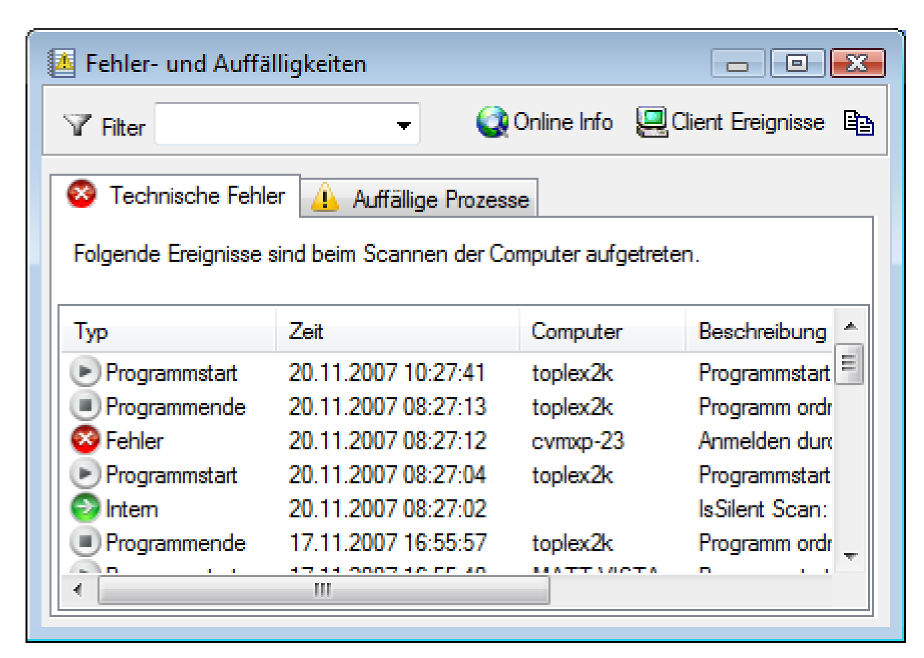
Ansehen des Fehlerprotokolls

Eine Übersicht über die aufgetretenen technischen Fehler finden Sie im Logbuch.

1. Klicken Sie in der Programm Symbolleiste auf



2. Sie sehen nun die aufgetretenen Fehler (z.B. Verbindungsprobleme).



Filter bestimmt einen Computer. Es werden nur Fehler angezeigt, die bei diesem Computer auftraten.

Online Info ermöglicht es, Online Hilfe zu dem speziellen Fehler zu erhalten.

Client Ereignisse zeigt die lokale Ereignisanzeige des gerade markierten Computers. Hierzu wird die Windows Ereignisanzeige gestartet. Der Remoteregistrierungsdienst muss auf dem Client aktiv sein und Sie (d.h. der gerade angemeldete Benutzer) müssen Admin-Rechte auf dem Client haben.

Anmerkung

- Um das Ereignisprotokolls eines beliebigen Clientcomputers zu sehen, klicken Sie mit der rechten Maustaste auf den gewünschten Computer in der Computerliste der Console. Klicken Sie dann auf **Ereignisprotokoll ▸**

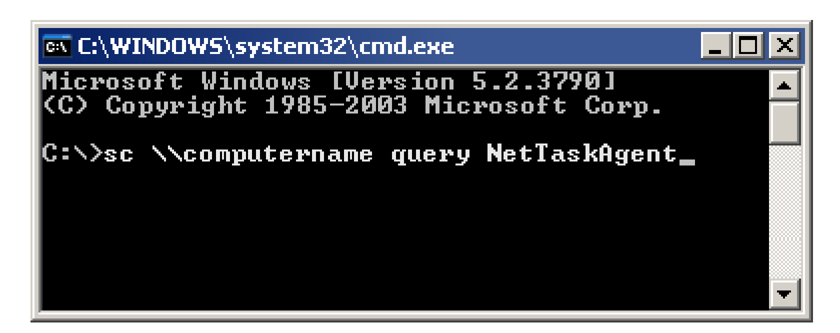
Technischer Support

Falls Sie in den FAQ 40 keine Lösung für Ihr Problem finden, so schreiben Sie uns bitte:

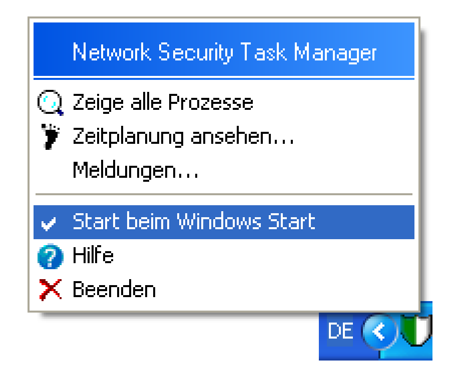
Anschrift: A. & M. Neuber Software GmbH
PF 11 05 25
D-06019 Halle
Fax: (+49) 0700-11 777 000
email: info@neuber.com
WWW: www.neuber.com/network-taskmanager

Zeitplanung/Warnung funktioniert nicht

Um vom Admin-PC aus zu überprüfen, ob auf einem Client der Agent-Dienst läuft, klicken Sie entweder im Computer-Eigenschaften 13 auf Jetzt testen oder führen den Befehl **sc \\ *computername* query nettaskagent** aus. Hierbei ist *computername* der Computername oder die IP-Adresse des Arbeitsplatzrechners im Netzwerk.



NetTaskTray 31 steuert Zeitplanung und Warnungen. Es muss deshalb im Infobereich der Taskleiste laufen. Um dies zu gewährleisten, können Sie die Option **Start beim Windows Start** aktivieren.



Administrator wird bei gefährlichen Prozessen nicht gewarnt
Haben Sie in der Zeitplanung Beim Start eines Prozesses 15 oder Nach dem Booten des Clients 15 eingestellt, so muss auch auf dem Computer, auf dem die Zentralkomponente läuft, die Datei- und Druckerfreigabe aktiviert sein. Bei diesen beiden Zeitplänen wird die Zentralkomponente informiert, wenn ein potenziell gefährlicher Prozess gefunden wurde.

Zeitplanung wird nicht ausgeführt
Bei einer eingestellten Zeitplanung startet NetTaskTray 31 bei Auffälligkeiten oder zu gegebener Zeit die Zentralkomponente/Console. Diese scannt dann den entsprechenden Computer. NetTaskTray muss in einem Benutzerkonto laufen, das Administrator-Rechte auf dem zu scannenden Computer hat.
Hintergrund: Ein Programm (hier NetTaskTray) mit eingeschränkten Rechten darf kein Programm mit höheren Rechten starten (z.B. die Zentralkomponente mit Admin-Rechten). Auch bei der Erweiterten Zeitplanung 15 müssen Sie ein Administratorkonto angeben.

Network Security Taskmanager unter einem anderen Benutzerkonto starten
Wenn Sie die Zentralkomponente mit einem anderen Benutzernamen (Windows Anmeldenamen) starten, so kann es passieren, dass Sie die Computer nicht mehr scannen können, auf denen schon der Agent-Dienst installiert ist.
Hintergrund: Benutzer A legt für einen Computer einen Zeitplan Beim Start eines Prozesses 15 oder Nach dem Booten des Clients 15 an. Der Agent-Dienst (300 KB) wird dann auf diesem Computer dauerhaft installiert. Aus Sicherheitsgründen kann der Agent-Dienst nur von Benutzer A kontaktiert und gesteuert werden. Später kann die Berechtigung noch geändert werden.

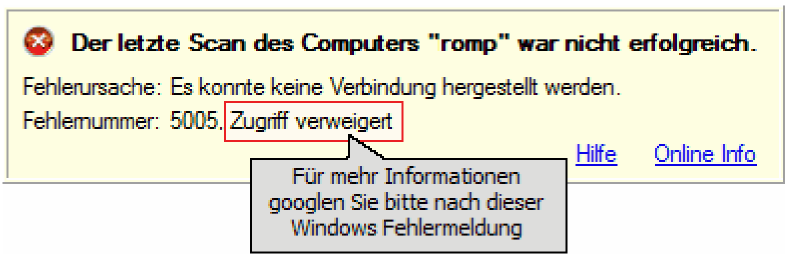
Anmerkung

- Klicken Sie im Menü **Ansicht** auf **Fehlerprotokoll** 42, um eine Übersicht aller bisher aufgetretenen technischen Fehlern zu sehen.

Fehlermeldungen

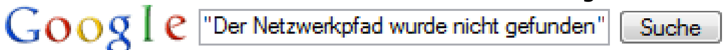
Finden der Fehlerursache anhand der Fehlermeldung

1. Wenn eine **Fehlermeldung** erscheint, so sehen Sie hinter der Fehlernummer, die von Windows herausgegebene Fehlermeldung.



2. Einige Fehlermeldungen:
   - Der Netzwerkpfad wurde nicht gefunden 44
   - Kein Zugriff auf die Dienste des Computers 44
   - Der RPC Server ist nicht verfügbar 44
   - Der angegebene Netzwerkpfad wurde von keinem Netzwerkdienstanbieter angenommen 44
   - Mehrfache Verbindungen zu einem Server ... sind nicht zulässig. 47
   - Dieser Netzwerkordner ist zurzeit unter Verwendung eines anderen Namens und Kennwortes verbunden. 47
   - Benutzer <Benutzername> hat keine Administrator Rechte auf <Clientcomputer> 47

3. Suchen Sie nach der markierten Fehlermeldung im Internet



Anmerkung

- Klicken Sie im Menü **Ansicht** auf **Fehlerprotokoll...** 42, um eine Übersicht aller bisher aufgetretenen technischen Fehlern zu sehen.

Fehler beim Verbinden

Fehlermeldungen:

- **Der Netzwerkpfad wurde nicht gefunden**
- **Kein Zugriff auf die Dienste des Computers**
- **Der RPC-Server ist nicht verfügbar**
- **Der angegebene Netzwerkpfad wurde von keinem Netzwerkdienstanbieter angenommen**

Ursachen & Lösungen:

Computer nicht erreichbar
Beim Anmelden auf dem zu scannenden Computer konnte der DNS- oder NetBIOS-Name nicht aufgelöst werden.

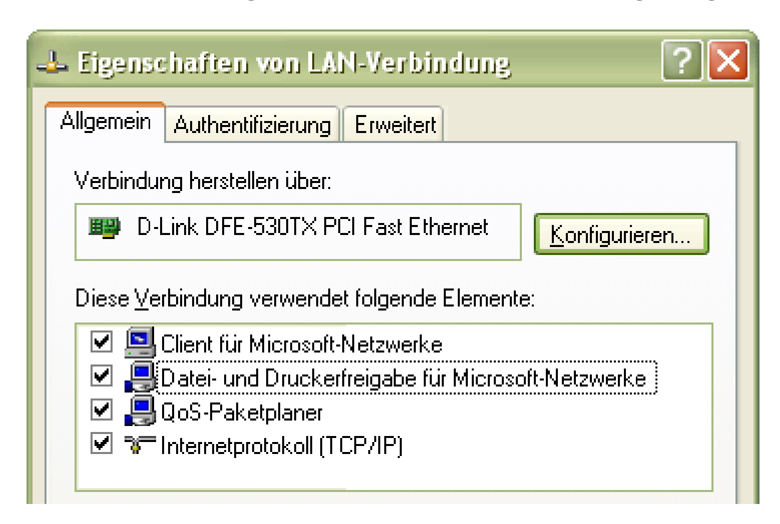
Lösung:

1. Vergewissern Sie sich, das der Computer existiert (Tippfehler im Computernamen?)
2. Vergewissern Sie sich, dass der Computer hochgefahren ist.
3. Überprüfen Sie, ob der Computer im Netzwerk erreichbar ist. Geben Sie z.B. in der Eingabeaufforderung (Start > Alle Programme > Zubehör > Eingabeaufforderung) den Befehl **`ping zielrechner`** ein.
4. Möglichweise ist in Ihrem Netzwerk *NetBIOS über TCP/IP* aktiviert, auf dem Remotecomputer wird jedoch der TCP-Port 139 durch die Firewall geblockt. Wenn Sie den Port 139 in der Firewall öffnen, so funktioniert die Namensauflösung wieder. Wenn Sie den Zielrechner anpingen können, funktioniert die Verbindung mit der IP-Adresse anstelle des Computernamens.

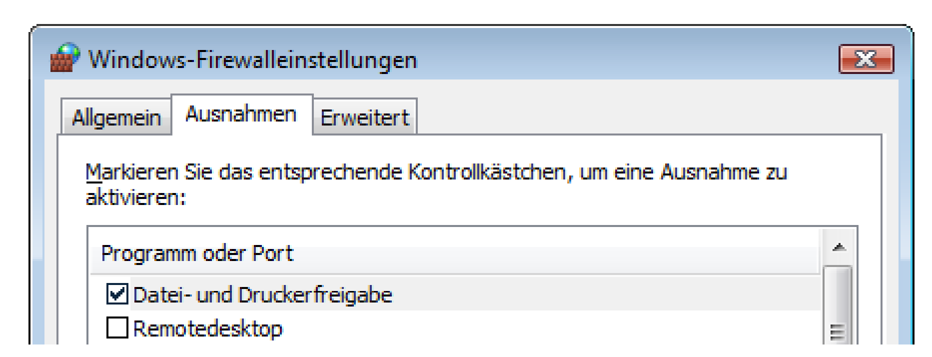
Datei- und Druckerfreigabe nicht aktiviert
Die "Datei- und Druckerfreigabe für Microsoft-Netzwerke" ist auf dem zu scannenden Computer nicht aktiviert bzw. durch Firewall geblockt.

Lösung:

1. Aktivieren Sie auf dem zu scannenden Computer die "Datei- und Druckerfreigaben für Microsoft-Netzwerke" in der Systemsteuerung > Netzwerkverbindungen > rechter Mausklick auf die gewünschte LAN-Verbindung > Eigenschaften



2. Die Firewall auf dem zu scannenden Computer darf die Datei-und Druckerfreigabe nicht blockieren. Das heißt der TCP-Port 445 (SMB Protokoll) muss offen sein.



Da die obigen Fehlermeldungen von einem allgemeinen Netzwerkproblem hervorgerufen werden, können Sie die Ursache auch mit Bordmitteln finden:

per Befehle in der Eingabeaufforderung

1. Öffnen Sie die Eingabeauforderung (Start > Alle Programme > Zubehör > Eingabeauforderung).
2. Geben Sie ein: **`ping Zielcomputer`**
   Kann ping den Zielcomputer nicht finden, so googeln Sie bitte nach der von ping ausgegebenen Fehlermeldung. Damit finden Sie Lösungsvorschläge. Vergewissern Sie sich, dass der Computername korrekt geschrieben und der Zielcomputer hochgefahren ist.
3. Geben Sie ein: **`runas /user:administrator cmd`**
   Hierbei ist **`administrator`** ein Administratorkonto auf dem Zielcomputer (z.B. admin oder domain\administrator). Diesen Benutzernamen geben Sie auch in der Login-Abfrage von Network Security Taskmanager an.
3. Geben Sie in der neu gestarteten Eingabeaufforderung ein: **`net view \\Zielcomputer`**. Anhand der ausgegebenen Fehlermeldung erkennen Sie die Fehlerursache:
   Es sind keine Einträge in der Liste oder
   Freigegebene Ressourcen auf \\Zielcomputer
   Datei- und Druckerfreigabe ist aktiviert.
   Gehört der Zielcomputer keiner Domäne an, sondern einer Arbeitsgruppe, so deaktivieren Sie auf diesem die Einfache Dateifreigabe 33!
   Systemfehler 5 ist aufgetreten. Zugriff verweigert
   Der im Schritt 2 verwendete Benutzername ist kein Administratorkonto auf dem Zielcomputer.
   Systemfehler 53 ist aufgetreten oder
   Systemfehler 51 ist aufgetreten
   Die "Datei- und Druckerfreigabe für Microsoft-Netzwerke" ist nicht aktiviert bzw. durch Firewall geblockt.

Lösungsvorschläge für tiefer liegende Netzwerkprobleme

1. Öffnen Sie auf dem zu scannenden Computer die Eingabeauforderung (Start > Alle Programme > Zubehör > Eingabeauforderung).
2. Geben Sie den Befehl **`net start rpcss`** ein.
   Überprüfen Sie, ob das Problem dadurch behoben wird. Tritt das Problem immer noch auf, gehen Sie weiter zum nächsten Schritt.
3. Geben Sie den Befehl **`ping zielrechner`** ein, wobei *zielrechner* der Server-, NetBIOS-, DNS- oder GUID-Name ist, dessen Verbindung Sie testen wollen.
4. Besteht ein Verbindungsproblem bei einem dieser Computer, geben Sie an der Eingabeaufforderung **netdiag** (Bestandteil des Microsoft Windows 2000 Resource Kit's) ein um zu bestimmen, ob der Domänencontroller korrekt arbeitet.
5. Wenn der Servername nicht korrekt aufgelöst wird, überprüfen Sie die DNS-Konfiguration des Domänencontrollers. Tritt das Problem immer noch auf, gehen Sie weiter zum nächsten Schritt.
6. Geben Sie an der Eingabeaufforderung **netdom** (Bestandteil des Microsoft Windows 2000 Resource Kit's) ein, um die Netzwerk-Vertrauensstellungen zu überprüfen und eine Verbindung zu einem Server zurückzusetzen oder einzurichten.
7. Wenn der primäre Domänencontroller für die Domäne nicht gefunden werden kann, wird der Domänenname nicht korrekt aufgelöst, überprüfen Sie die DNS-Konfiguration des Domänencontrollers.

Anmerkung

- Der RPC Server wird von Network Security Taskmanager nicht remote gesteuert. Somit kann der Port 135 aus Sicherheitsgründen stets geschlossen bleiben.
- Mit dem Befehl **`netdiag /debug`** lassen sich generelle Netzwerk-Fehler aufspüren.
  Mit **`netdiag /fix`** lassen sich einfachere Fehler schnell beheben. Danach kann man auch noch mit dem Tool **`dcdiag`** die Fehlersuche fortsetzen.

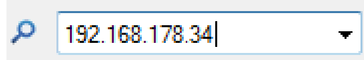
Mehrfache SMB Verbindungen

Fehlermeldungen:

- **Mehrfache Verbindungen zu einem Server oder einer freigegebenen Ressource von demselben Benutzer unter Verwendung mehrerer Benutzernamen sind nicht zulässig. Trennen Sie alle früheren Verbindungen zu dem Server bzw. der freigegebenen Ressource, und versuchen Sie es erneut.**
- **Dieser Netzwerkordner ist zurzeit unter Verwendung eines anderen Namens und Kennwortes verbunden. Trennen Sie zuerst jede bestehende Verbindung auf diese Netzwerkfreigabe, um unter Verwendung eines anderen Namens und Kennwortes verbunden zu werden.**

Ursache:
Zu dem zu scannenden Computer besteht schon eine Netzwerkverbindung (SMB Protokoll) unter einem anderen Benutzernamen ohne Administrator Rechte. Windows lässt es leider nicht zu, eine weitere Verbindung mit anderem Benutzerkonto aufzubauen.

Lösung A:
Verwenden Sie bitte im Network Security Taskmanager die IP-Adresse anstatt des Computernamens.



Lösung B:
Öffnen Sie den Windows Explorer auf dem zu scannenden Computer. Klicken Sie im Menü **Extras** auf **Netzlaufwerk trennen**. Trennen Sie nun die bestehende Verbindung.

Lösung C:

1. Öffnen Sie auf dem zu scannenden Computer die Eingabeaufforderung (Start > Alle Programme > Zubehör > Eingabeaufforderung).
2. Führen Sie dann den Befehl **`net use`** aus, um zu sehen welche Verbindungen bestehen.
3. Mit **`net use /delete <entsprechende Verbindung>`** beenden Sie die jeweilige Verbindung (egal ob als Status "getrennt" steht oder nicht). Sie können aber auch mit dem Befehl **`net use * /delete`** alle Verbindungen trennen.

Keine Admin-Rechte

Fehlermeldungen:

- **Benutzer <Benutzername> hat keine Administrator-Rechte auf <Clientcomputer>**

Ursachen & Lösungen:

Zielrechner mit Windows 8/7/Vista
Bitte beachten Sie folgende Hinweise, wenn Sie einen Computer scannen möchten, auf dem **Windows 8/7/Vista** läuft und der sich **in einer Arbeitsgruppe** befindet.

Gehört der zu scannende **Windows 8///Vista** Computer keiner Domäne an, sondern einer **Arbeitsgruppe**, so verhindert die Benutzerkontensteuerung (UAC), dass *Network Security Taskmanager* kurzzeitig einen Agent in die administrative Freigabe admin$ installieren kann.

Lösung:
Nehmen Sie auf dem zu scannenden Arbeitsgruppen-Computer eine kleine Anpassung 34 vor oder installieren Sie den Agent dauerhaft.

Das angegebene Benutzerkonto ist kein Administratorkonto
Wenn Network Security Taskmanager den Clientcomputer scannt, so werden Sie nach Benutzername und Kennwort eines Administrator-Accounts auf dem zu scannenden Clientcomputer gefragt. Die Login-Daten, welche Sie eingegeben haben, gehören jedoch zu keinem Administrator-Konto auf dem zu scannenden Clientcomputer.

Lösung:
Vergewissern Sie sich, dass Sie Benutzername und Kennwort richtig eingegeben haben und dass dieser Benutzer Admin Rechte auf dem zu scannenden Clientcomputer hat.

Einfache Dateifreigabe ist aktiviert
Auf dem zu scannenden Clientcomputer ist die "Einfache Dateifreigabe" aktiviert und der Zielcomputer gehört einer **Arbeitsgruppe** an.

Lösung:
Deaktivieren Sie auf dem Clientcomputer die Einfache Dateifreigabe 33.

Als Nicht-Admin Network Security Taskmanager per Zeitplanung starten
Wenn Network Security Task Manager nicht unter einem Administrator-Account laufen darf, erfolgt immer eine Passwort Abfrage beim Scan. Wie kann man aber den Zielcomputer per Zeitplanung scannen?

Lösung:
Aus Sicherheitsgründen ist es nicht möglich, dass sich Network Security Taskmanager Passwörter merkt. Dies ist nur innerhalb einer Windows Sitzung möglich. Nach einem Neustart muss also immer das Admin-Passwort des Zielrechner neu eingetragen werden. Am einfachsten wäre es also den Windows Rechner ständig laufen zu lassen.

Statt dem unsicherem **runas: /user:Administrator /savecred "C:\..\"** lieber **runasspc** verwenden:

- Es wird nicht nur eine Prüfsumme in der verschüsselten Datei angelegt, sondern ein ganzes Bitmuster des freigegebenen Programmes wird verschlüsselt abgelegt und beim Aufruf gegengeprüft.
- Der Schlüssel wird zur Laufzeit aus der ausführbaren Datei, zusammen mit einem errechneten Passwort erzeugt. Jede Anwendung erhält dadurch einen eigenen Schlüssel kombiniert mit enem festen Schlüssel. Beide Schlüssel stehen deshalb auch nicht irgendwo fest codiert.
- Das Tool wurde nach Vorgaben ursprünglich für eine Firma entwickelt welche sich an BSI Normen hält.

Desweiteren sind für Sie folgende Einstellungen (unter "Konfiguration") in Network Security Taskmanager wichtig (bitte dazu auch die Hilfe ansehen):
a) die Option "Auto-Modus"
b) Zeitplanung 15 > "Beim Start eines Prozesses"


Teil
VII

VII. Softwareverteilung per MSI-Paket

Überblick

Die Verteilung der Agenten 9 übernimmt Network Security Taskmanager automatisch. In großen Netzwerken kann der Agent jedoch auch dauerhaft per MSI-Paket verteilt werden. Das MSI-Paket enthält den schlanken Agenten (nur 300 KB groß), welcher auf dem zu überwachenden Computer verteilt wird (unbeaufsichtigte Installation). Das MSI-Paket kann nur mit einer Anpassung der Parameter verteilt werden. Ohne diese Anpassung funktioniert die Kommunikation zur Zentralkomonente nicht.

Die Anpassung der Parameter erfolgt entweder

- mit einer mst Datei
  Ideal für die Verteilung in größeren Netzwerken. Dieses Dokument beschreibt, wie die MST-Datei erstellt wird und zusammen mit der msi Datei im Netzwerk verteilt wird.

  So verteilen Sie den Agent-Dienst per msi

  1. Erstellen Sie eine Transformationsdatei (*.mst) 51.
  2. Speichern Sie MSI & MST Datei in einem freigegebenen Ordner 53.
  3. Verteilen Sie das Paket z.B. per Gruppenrichtlinie 55.

- **Übergabe per Parameter**
  Dies ist nützlich zu Testzwecken. Der Dateiname nettaskagent.exe des Agent-Dienstes kann hierbei jedoch nicht geändert werden.
  Mit folgendem Befehl wird die Installation (z.B. in der Eingabeaufforderungoder per Loginscript) gestartet:

```
msiexec /i "\\servername\share\NetTaskAgent.msi" INSTALLDIR="c:\myfolder"
SERVER="Servername" USER="Administrator" /qn
```

  Parameter

  INSTALLDIR gibt das lokale Verzeichnis auf dem Zielrechner an, in das die Agent Datei NetTaskAgent.exe kopiert wird. Wird der Parameter weg gelassen, so wird der Agent in das System32 Verzeichnis des lokalen Windows Ordners installiert. Dies entspricht der Standardeinstellung.

  SERVER gibt den Namen des Computers an, auf welchem NetTaskTray.exe läuft. Meistens befindet sich dort auch die Console. Den Computernamen sehen Sie z.B. in der Netzwerkumgebung.

  USER gibt den Benutzernamen (z.B.: Domäne\Benutzer) an, unter dem NetTaskTray.exe 31 läuft. Meistens läuft auch die Console in diesem Benutzerkonto. Ein Passwort muss nicht angegeben werden.

  /qn Zeigt keine Benutzeroberfläche an (unbeaufsichtigte Installation)
  Wenn Sie anstelle **/qn** den Parameter **/qb** nehmen, sehen Sie auf dem Client den Fortschritt der Installation.

Anmerkung

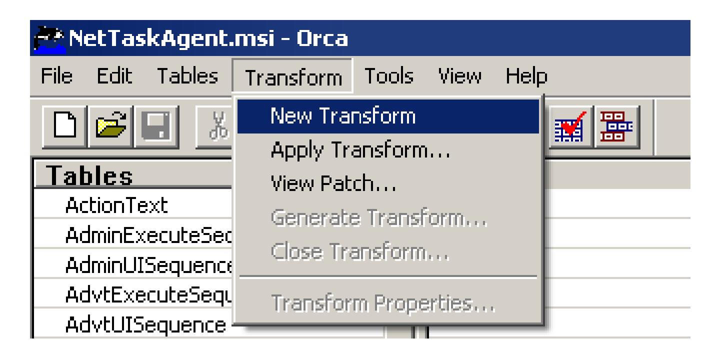
- Das MSI-Paket **NetTaskAgent.msi** für die Verteilung des Agenten befindet sich im Programmordner (z.B. in c:\Programme\Network Security Taskmanager\).
- Wird der Agent per MSI-Paket installiert, so erscheinen diese Computer erst im Programm, wenn der Agent einen potenziell gefährlichen Prozess meldet.

Erstellen der MST Datei

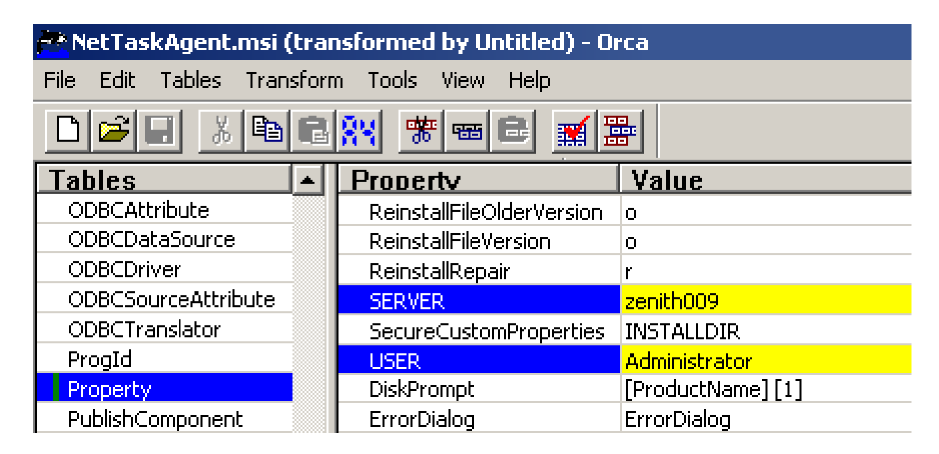
Die Datei custom.mst kann mit dem kostenlosen Tool **ORCA** erstellt werden.
Download: http://www.neuber.com/network-taskmanager/deutsch/docs/orca.html

1. Starten Sie ORCA und öffnen Sie die Datei **`NetTaskAgent.msi`**. Die Datei befindet sich im Programmordner von Network Security Taskmanager.

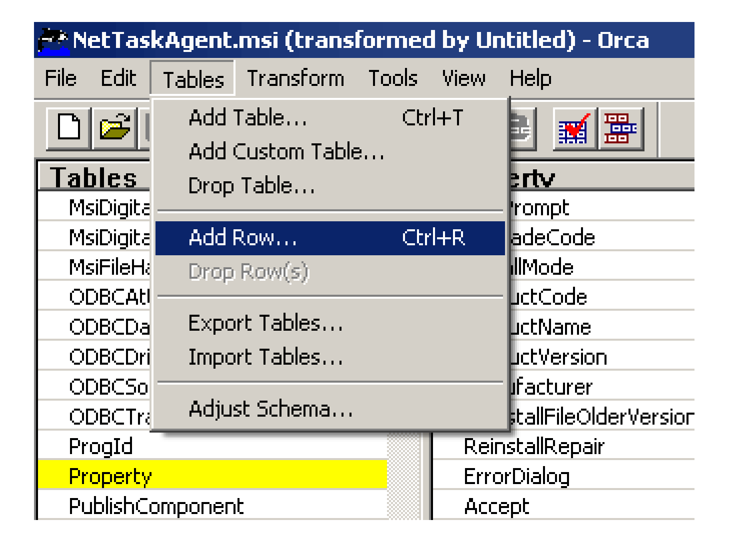
2. Klicken Sie im Menü **Transform** auf **New Transform**



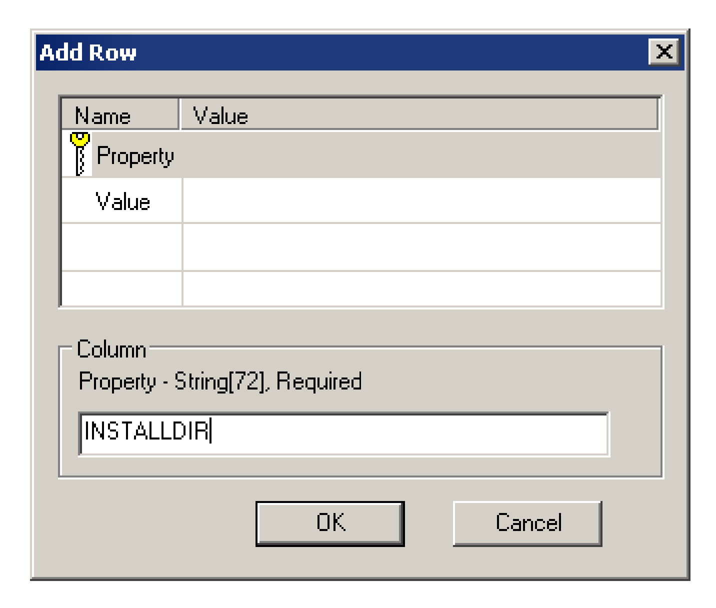
3. Klicken Sie in der Table-Liste auf **Property**. Geben Sie den Computernamen und das verwendete Benutzerkonto (z.B.: Domäne\Benutzer) von NetTaskTray.exe 31 an. Meistens läuft auch die Console 5 in diesem Benutzerkonto.



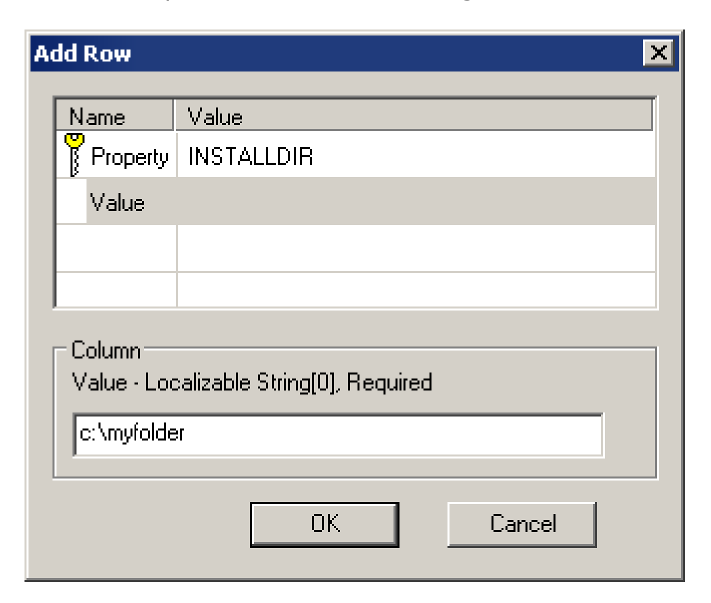
4. Die Datei wird standardmäßig in das lokale Windows\System32 des Arbeitsplatzrechners installiert. Optional kann auch ein beliebiger Ordner und Dateiname für die Agenten-Datei angeben werden:



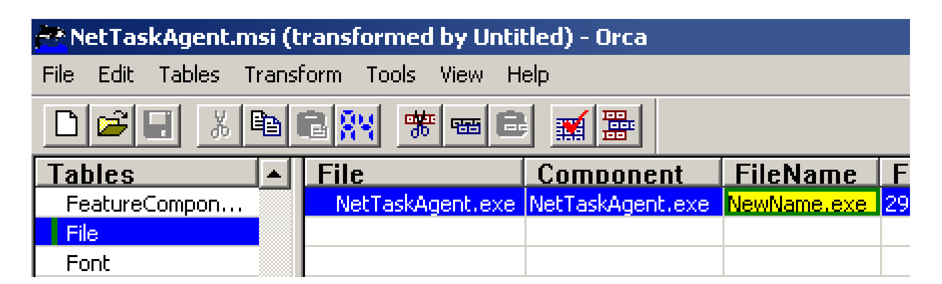
5. Geben Sie **INSTALLDIR** ein und drücken Sie die Enter Taste.



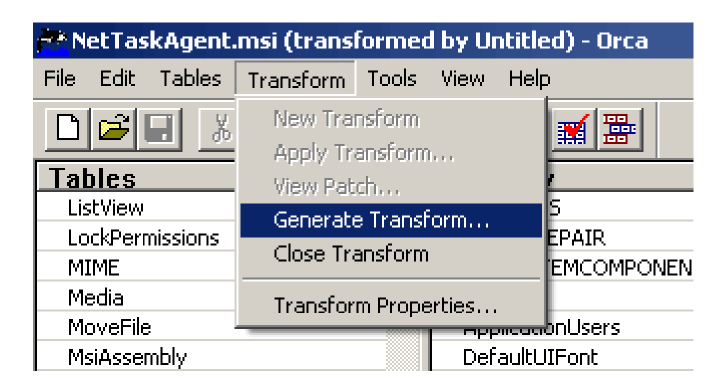
6. Geben Sie den lokalen Pfad des Arbeitsplatzrechners ein. Dorthin wird die NetTaskAgent.exe Datei später installiert. Bestätigen Sie mit OK oder Enter.



7. Klicken Sie auf die Table **File** und geben Sie in der Spalte FileName einen beliebigen Namen für die Datei an.



8. Klicken Sie im Menü **Transform** auf **Generate Transform...**

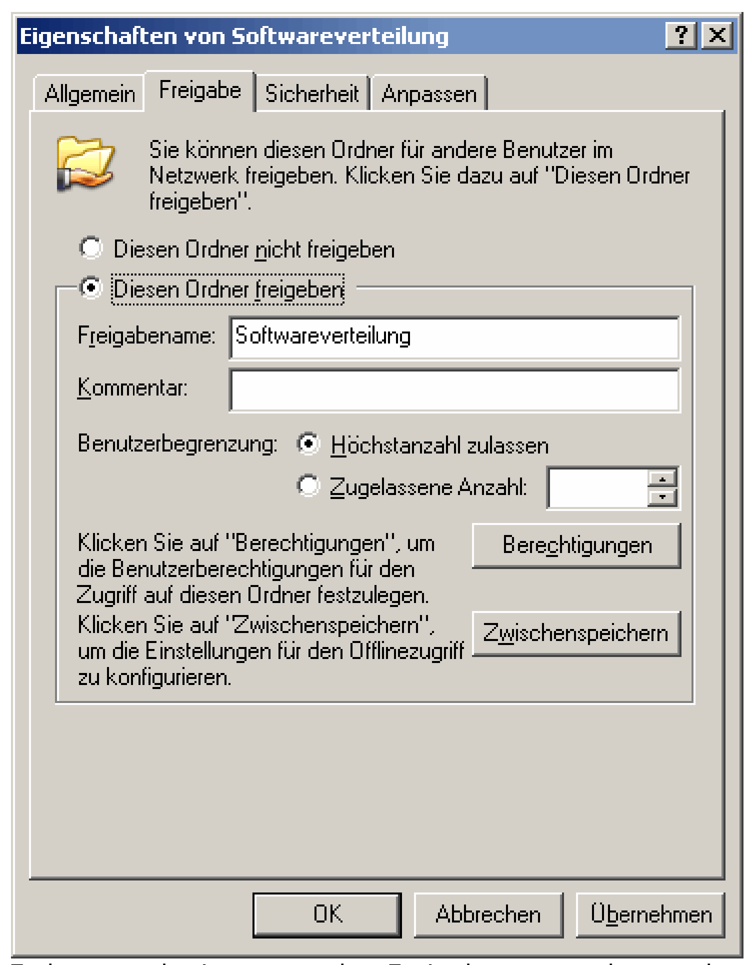


9. Speichern Sie die Datei unter dem Namen **`custom.mst`** ab.

Nächster Schritt:
Ablegen der MSI und MST Datei in einem freigegebenen Ordner 53

Anlegen eines Freigabe-Ordners

1. Verzeichnis auf Dateiserver (Domänenmitglied) oder Netzlaufwerk anlegen und freigeben.

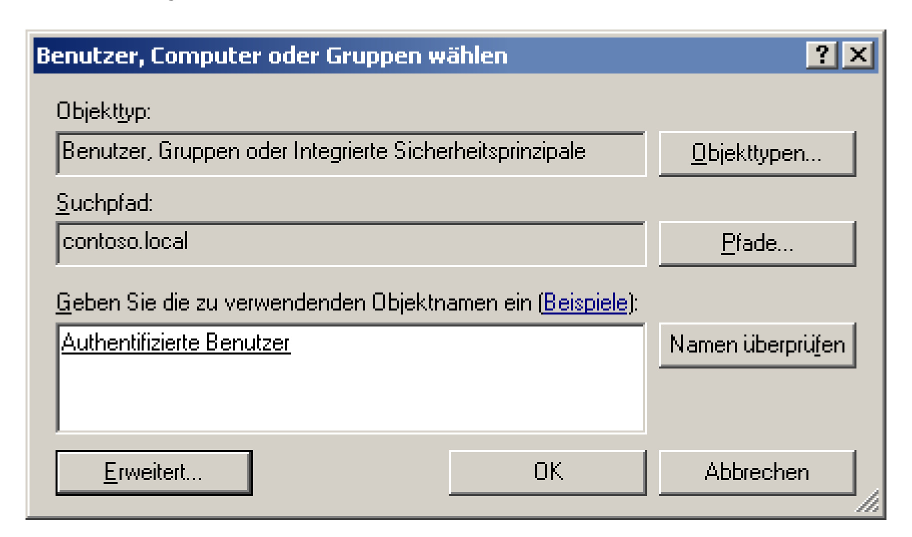


Es kann auch eine versteckte Freigabe verwendet werden. Hierzu wird dem Freigabenamen ein Dollarzeichen angehängt: *Softwareverteilung$*.

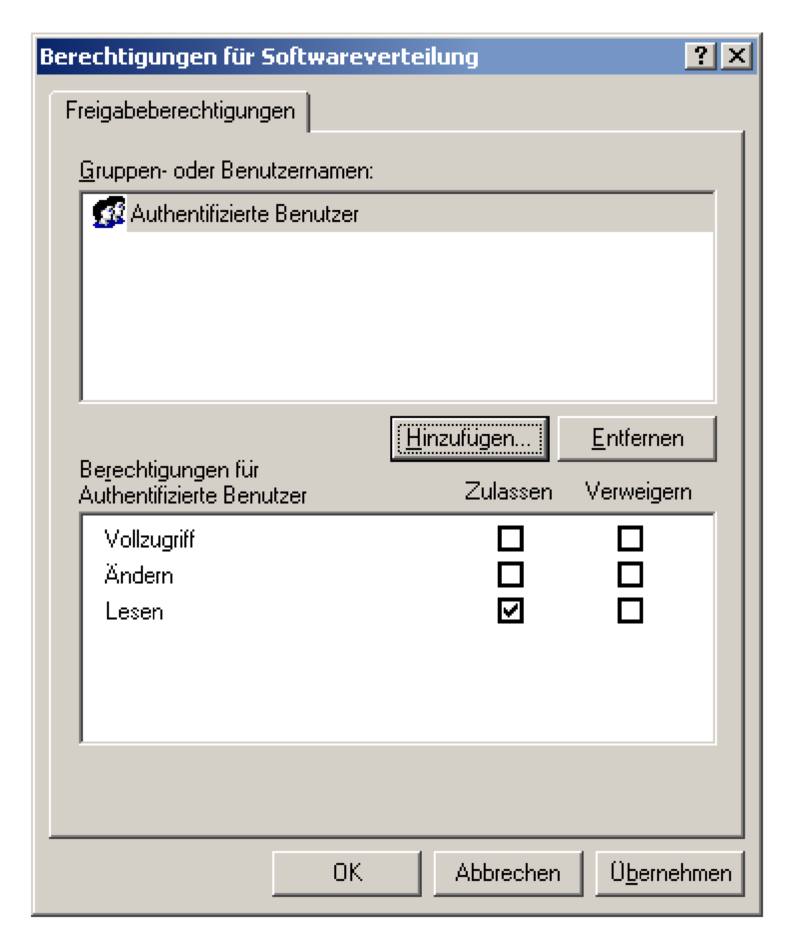
2. Klicken Sie auf **Berechtigungen**. Standardmäßig ist der Lesezugriff für **Jeder** gesetzt. Entfernen Sie diesen Benutzer.

3. Klicken Sie auf **Hinzufügen** und setzen Sie den Lesezugriff für Gruppe **Authentifizierte**

Benutzer. Mitglieder dieser vordefinierten Gruppe sind alle Computer- und Benutzerobjekte, die sich an der Domäne authentifiziert haben.



4. Klicken Sie auf **Erweitert**, dann auf **Jetzt suchen**. Wählen Sie dann **Authentifizierte Benutzer**. Klicken Sie **OK**.



5. Klicken Sie **OK**.

6. Kopieren Sie die Dateien NetTaskAgent.msi und custom.mst in den neu angelegten Ordner *Softwareverteilung*.

Nächster Schritt:
Die Softwareverteilung 55

Softwareverteilung per Gruppenrichtlinie

In großen Netzwerken wird die msi und mst Datei per Systemmanagement- bzw. Deployment-Software verteilt. Im Folgenden wird die Softwareverteilung per Script und per GPMC beschrieben:

Softwareverteilung per Script

Mit folgendem Befehl wird die Installation (z.B. in der Eingabeaufforderung oder per Loginscript) gestartet:

```
msiexec /i "\\servername\share\NetTaskAgent.msi" TRANSFORMS="\
\servername\share\custom.mst" /qn
```

Softwareverteilung unter Windows 2000 Server

Wenn Sie noch einen Windows Server 2000 betreiben, so können Sie mit den folgenden Schritten sehr einfach die NetTaskAgent.msi verteilen. Wir empfehlen jedoch die weiter unten beschriebene Anleitung per GPMC.

1. Klicken Sie im Startmenü auf Verwaltung > "Active Directory-Benutzer und -Computer".
2. Öffnen Sie mit einem Rechtsklick auf die gewünschte Computergruppe (OU) den Eigenschaften-Dialog.
3. Wählen Sie den Karteireiter **Gruppenrichtlinie**.
4. Erstellen Sie mit Neu eine neue Richtlinie namens "NetSTM-Dienst Installation". Öffnen Sie diese mit **Bearbeiten**.
5. Klicken Sie auf Computerconfiguration/Softwareeinstellungen. Dann mit Rechtsklick Neu > Paket.
6. Öffnen sie die Datei \\servername\share\NetTaskAgent.msi.
7. Klicken Sie auf die Option **Erweitert**.
8. Klicken Sie auf die Registerkarte **Änderungen**. Dann Klicken Sie auf **Hinzufügen**, um die Datei custom.mst hinzuzufügen.
9. Klicken Sie auf die Registerkarte **Bereitstellung von Software**. Aktivieren Sie die Option: "*Anwendung deinstallieren, wenn sie außerhalb des Verwaltungsbereichs liegt*"
10. Bestätigen Sie die Änderungen mit **OK**.
    Beim nächsten Neustart der Clientrechner in dieser Computergruppe (OU) wird vor der Anmeldung des Nutzers der Agent-Dienst installiert.

Empfohlende Vorgehensweise für die Verteilung per Gruppenrichtlinien

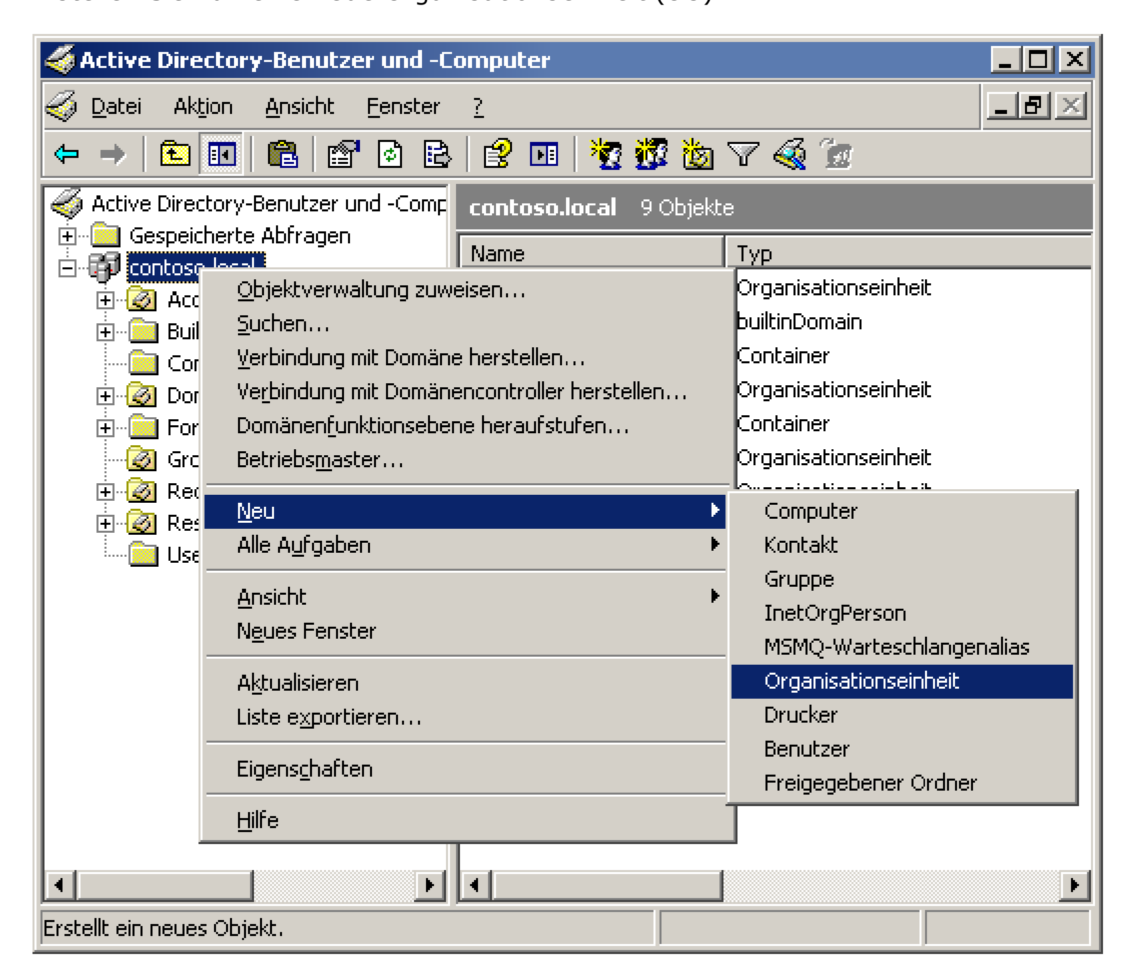
Für Windows Server 2003/2008 und alle aktuellen Betriebssysteme empfiehlt sich die Gruppenrichtlinienverwaltung (kurz: GPMC) (Download: http://www.microsoft.com/downloads/details.aspx?familyid=F39E9D60-7E41-4947-82F5-3330F37ADFEB&displaylang=de)

Um die Gruppenrichtlinienverwaltung auf einen Client eines Administrators nutzen zu können, muss vorher das Administration Tools Pack installiert werden: http://www.google.de/search?hl=de&&q=windows+server+Administration+Tools+Pack

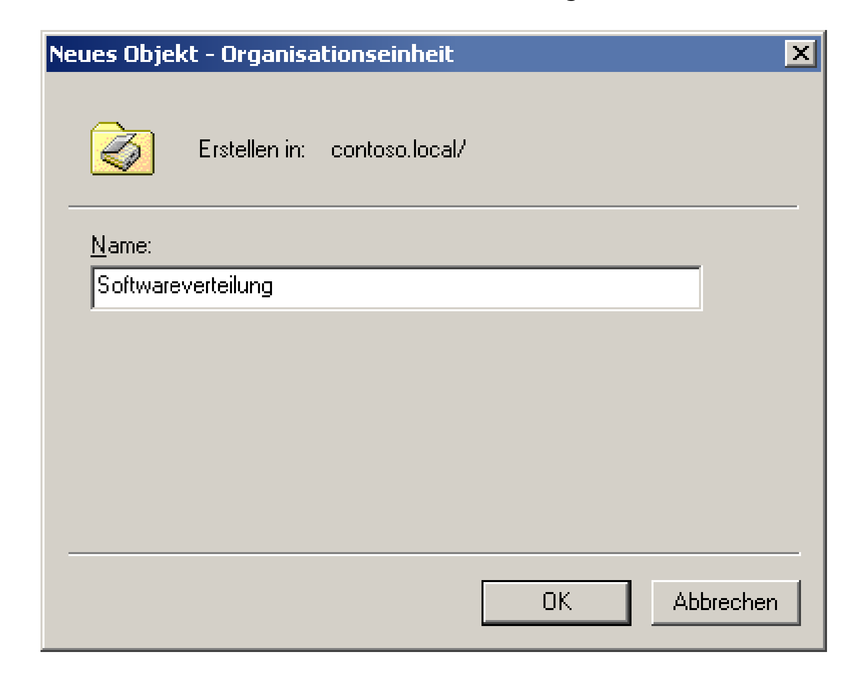
A) Sicherheitsgruppe einrichten

Die Sicherheitsgruppe enthält später alle Computer, auf welchen der Agent-Dienst installiert wird.

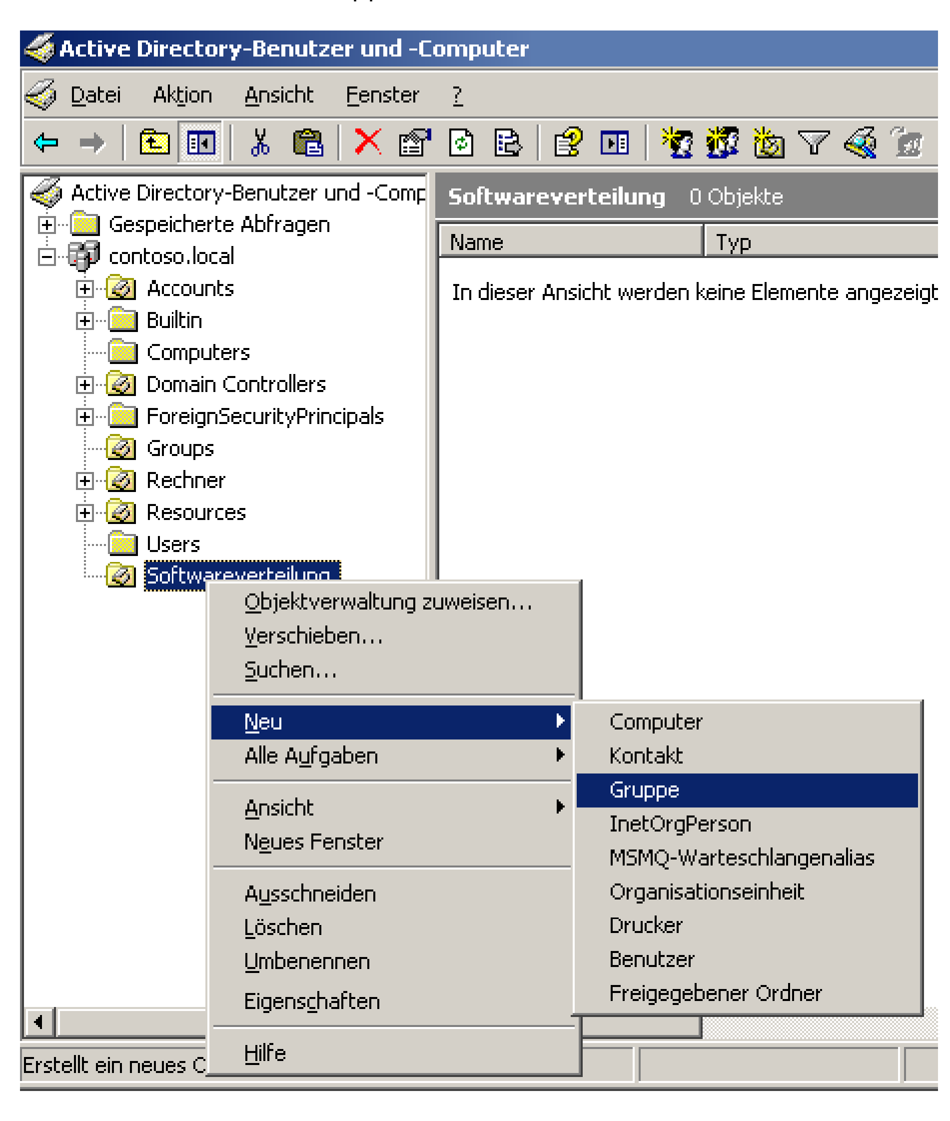
1. Klicken Sie im Startmenü auf Verwaltung > "Active Directory-Benutzer und -Computer". Erstellen Sie nun eine neue Organisationseinheit (OU).



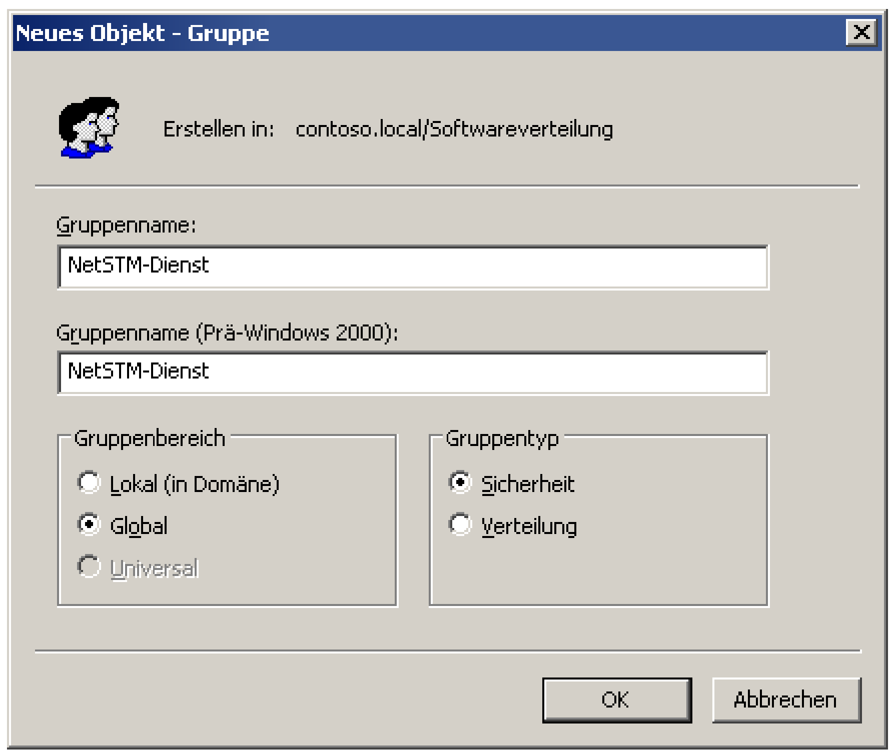
2. Nennen Sie die OU z.B. "Softwareverteilung".



3. Erstellen Sie eine neue Gruppe **NetSTM-Dienst** in der OU "Softwareverteilung".

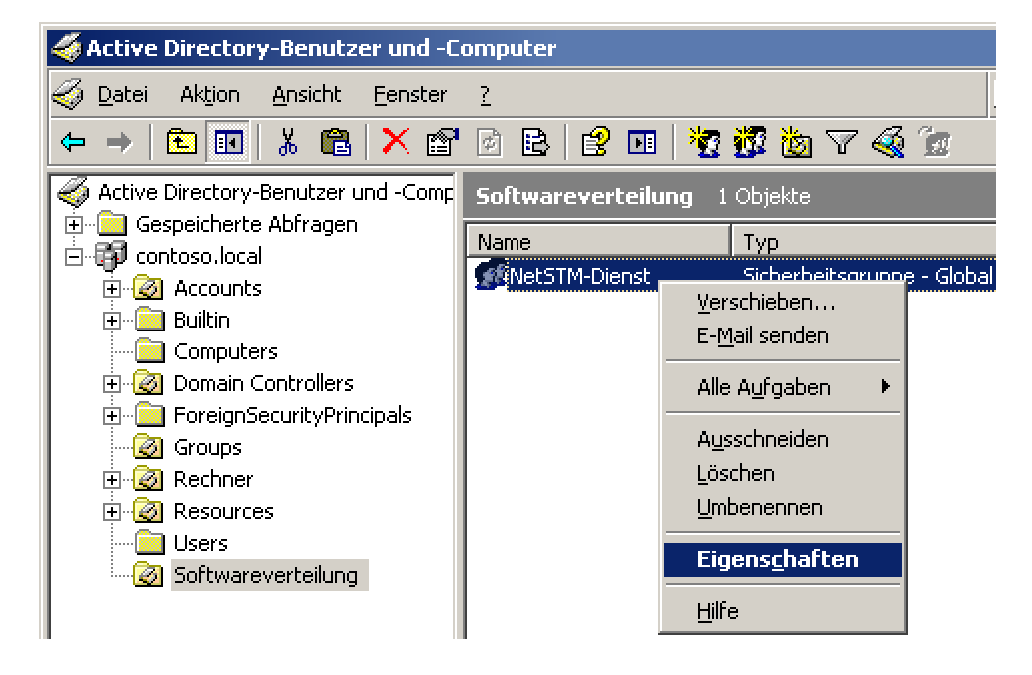


mit folgenden Parametern:

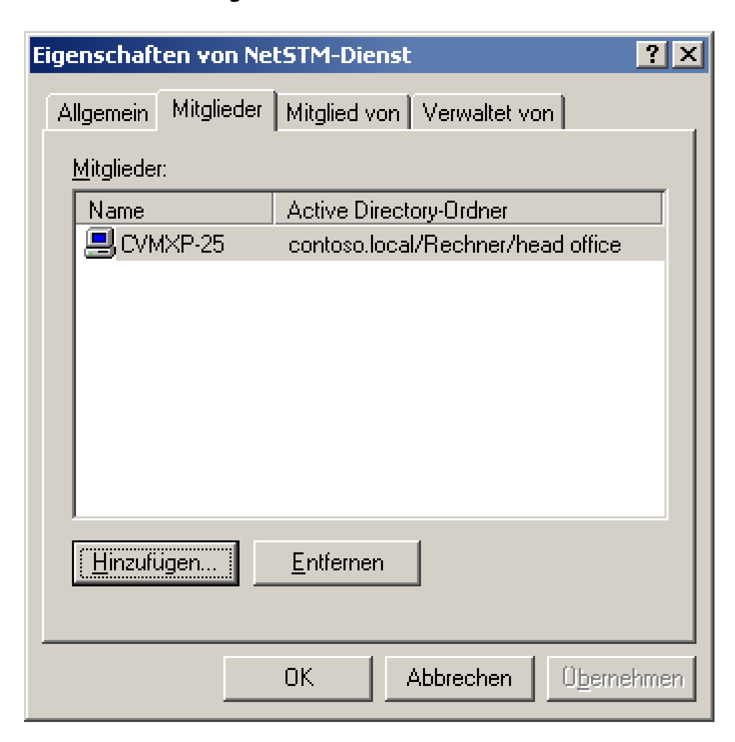


Klicken Sie auf **OK**.

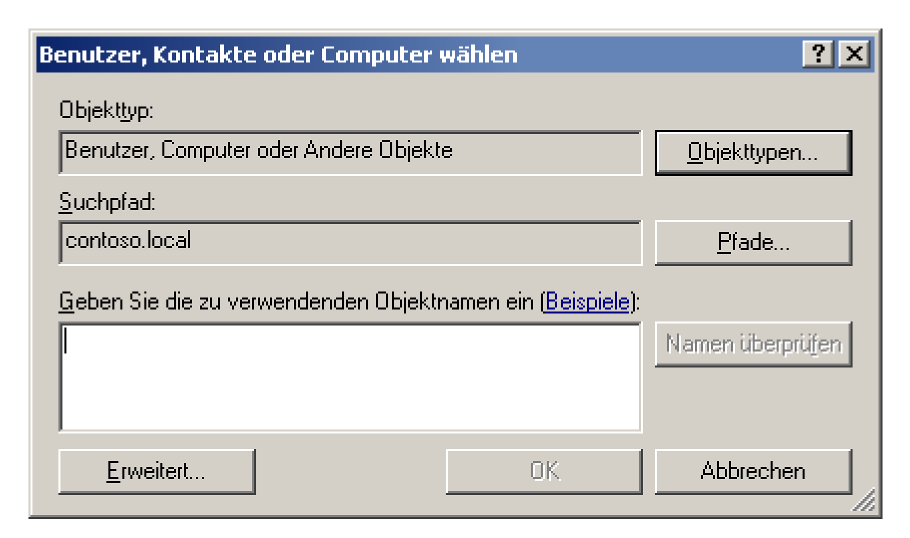
4. Doppelklicken Sie die neu erstellte Gruppe (bzw. Rechter Mausklick -> Eigenschaften)



5. Klicken Sie auf **Hinzufügen**, um die Computer zu wählen, auf welchen später der NetSTM-Dienst NetTaskAgent.msi installiert werden soll.



Tipp: Klicken Sie auf "**Objekttypen...**", um sich zu vergewissern, dass auch Computer angezeigt werden. Klicken Sie auf den Button "**Erweitert...**" und dann auf "**Jetzt suchen**", um die verfügbaren Clients zu sehen.

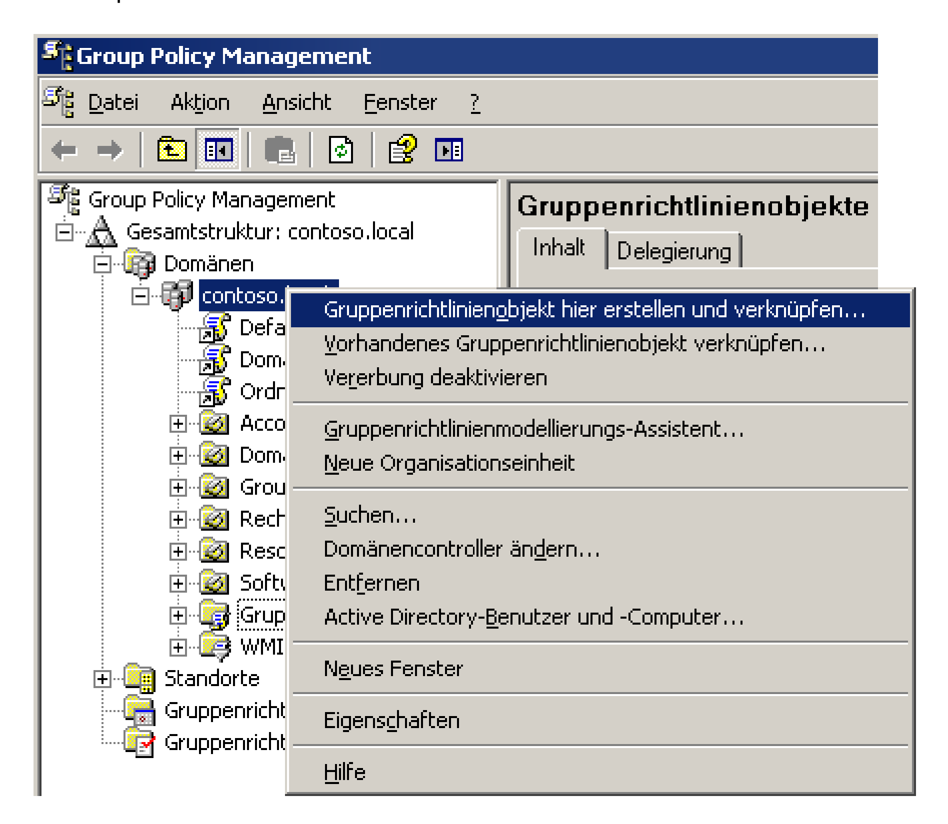


Klicken Sie anschließend auf **OK**, um die gewählten Computer zu übernehmen.

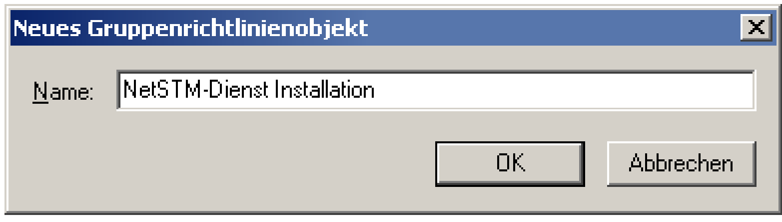
B) Erstellen der Gruppenrichtlinie

1. Starten Sie die Gruppenrichtlinienverwaltung. Hierzu GPMC.msc ausführen oder klicken Sie in der Systemsteuerung bzw. im Startmenü auf Verwaltung > Gruppenrichtlinienverwaltung.

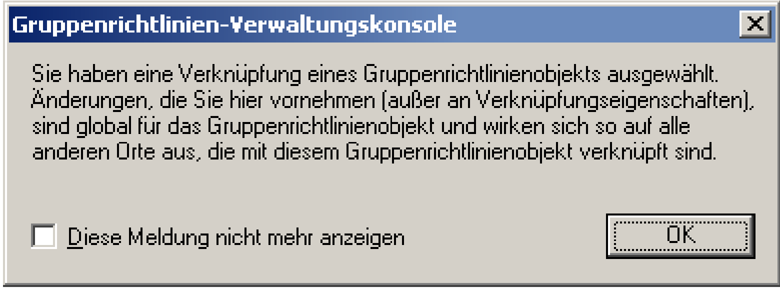
2. Klicken Sie mit der rechten Maustaste auf "Gruppenrichtlinenobjekt hier erstellen und verknüpfen...".



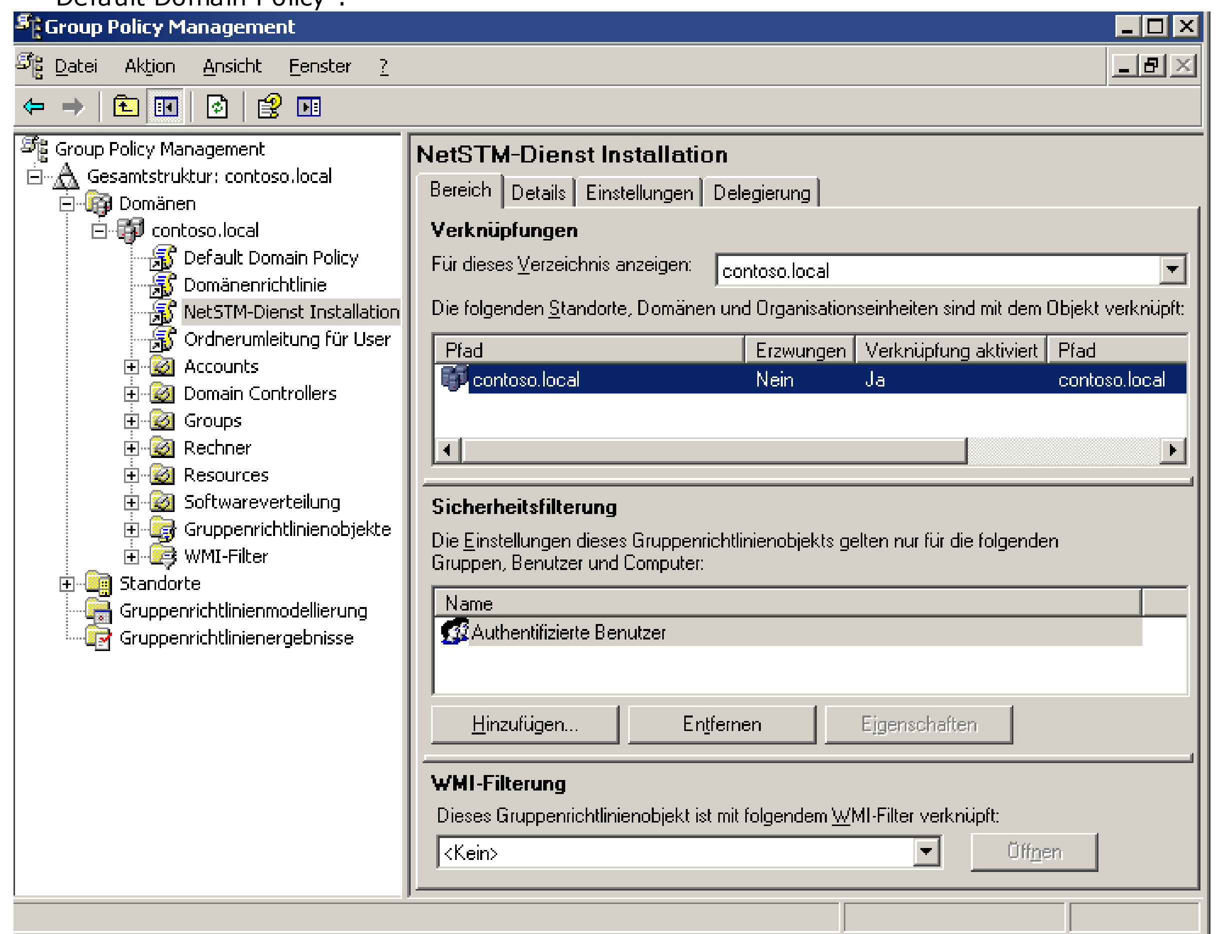
und wählen Sie einen bezeichnenden Namen



Bestätigen Sie die Abfrage

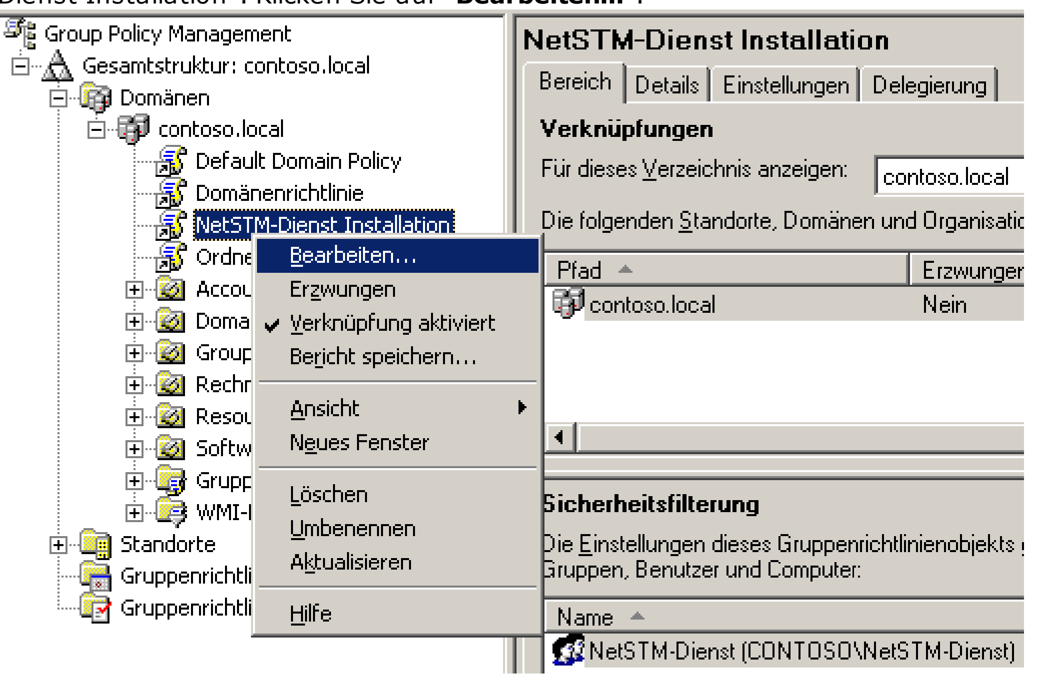


3. Nun erscheint die eben erstellte Gruppenrichtlinie unter dem Domain Namen und der "Default Domain Policy".

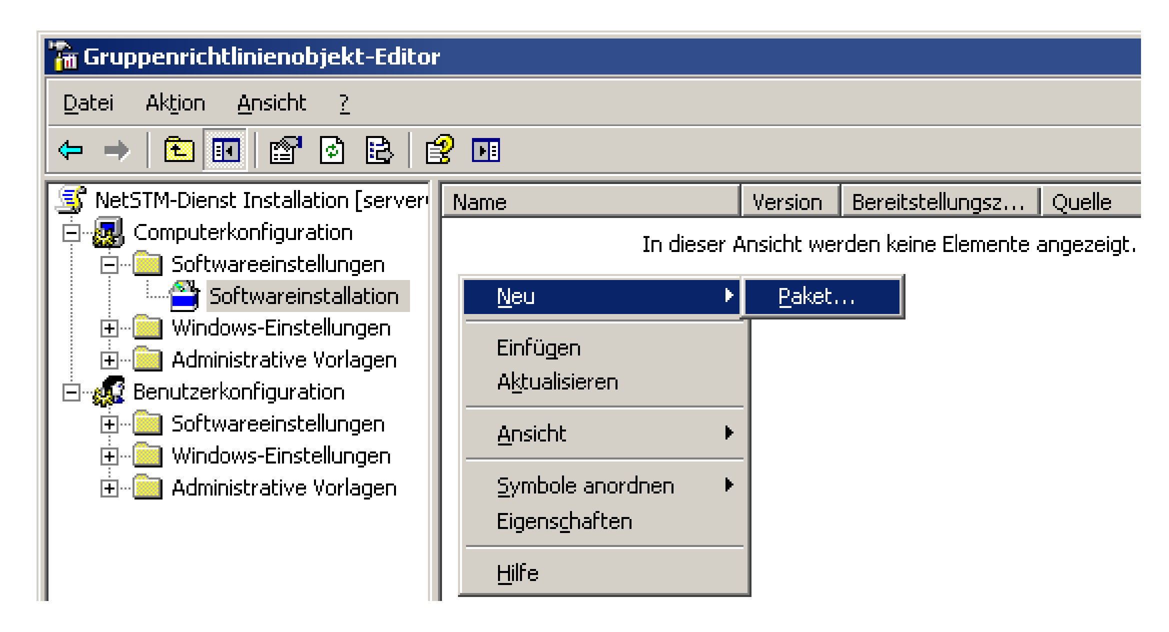


Entfernen Sie die Gruppe "Authentifizierte Benutzer" und fügen Sie über **Hinzufügen** die vorhin erstellte Sicherheitsgruppe "NetSTM-Dienst" hinzu. Damit ist der Wirkungsbereich dieser Gruppenrichtlinie auf die Sicherheitsgruppe "NetSTM-Dienst" beschränkt.

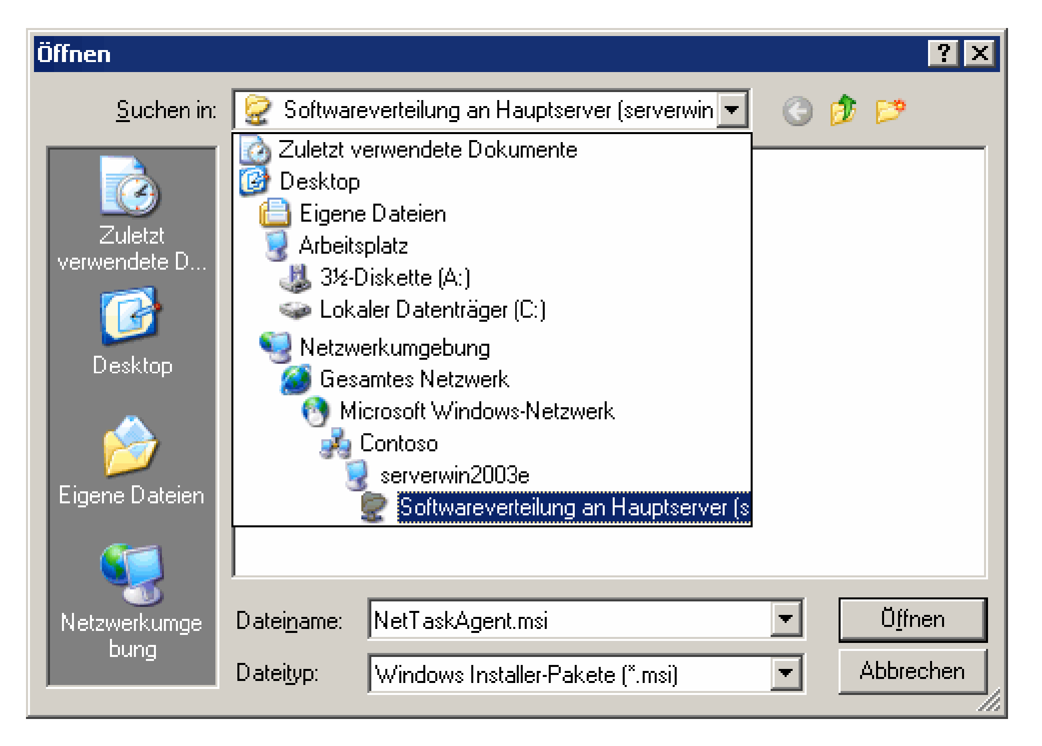
4. Klicken Sie mit der rechten Maustaste auf die eben erstellte Gruppenrichtlinie "NetSTM-Dienst Installation". Klicken Sie auf "**Bearbeiten...**".



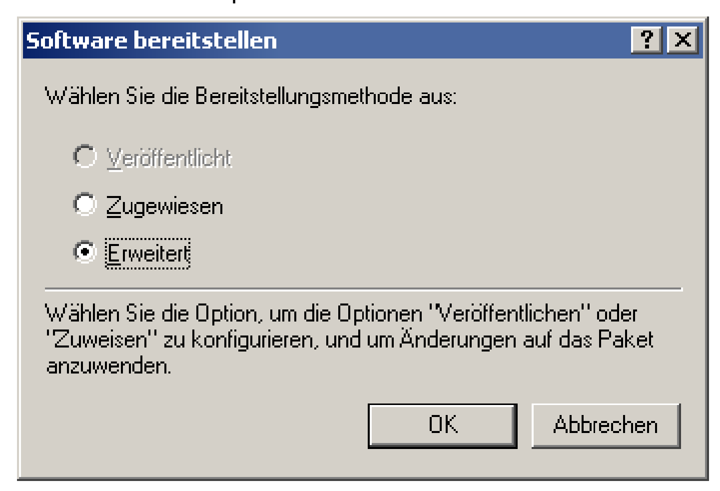
5. Im Gruppenrichtlinienobjekt-Editor klicken Sie unter Computerkonfiguration > Softwareeinstellungen > Softwareinstallation. Klicken Sie nun mit der rechten Maustaste auf den weißen Bereich.



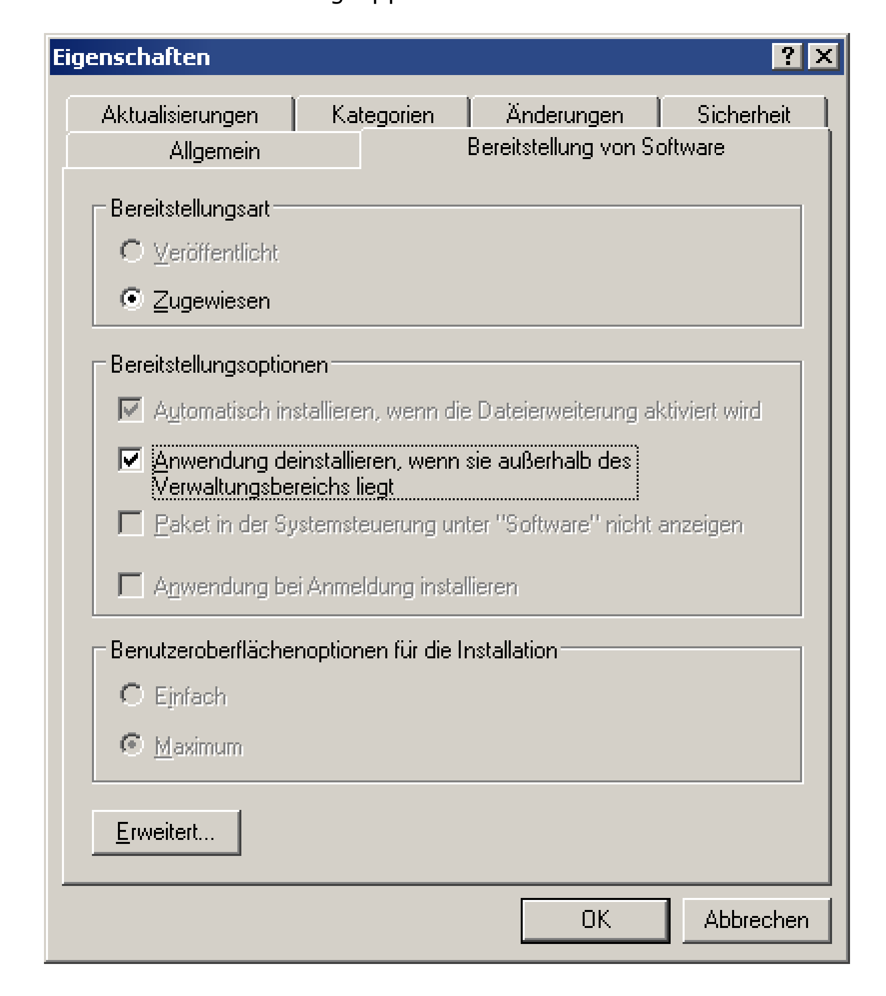
6. Wählen Sie das MSI-Paket mit UNC Pfad, also \\server\softwareverteilung\NetTaskAgent.msi



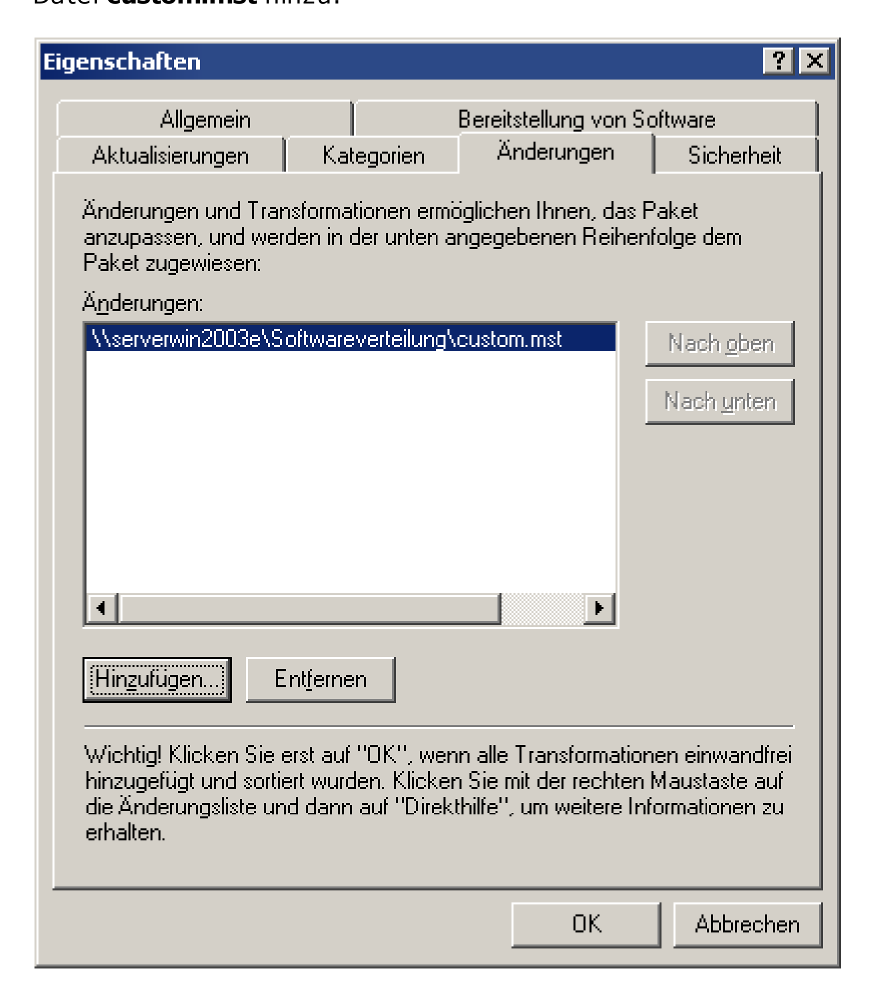
Wählen Sie die Option **Erweitert**.



7. Klicken Sie nun auf die Registerkarte **Bereitstellen von Software**. Aktivieren Sie die Option "Anwendung deinstallieren, wenn sie außerhalb des Verwaltungsbereichs liegt". Damit wird die Net-STM-Dienst Software automatisch wieder von einem Client deinstalliert, sobald man ihn aus der Sicherheitsgruppe "NetSTM-Dienst" entfernt.



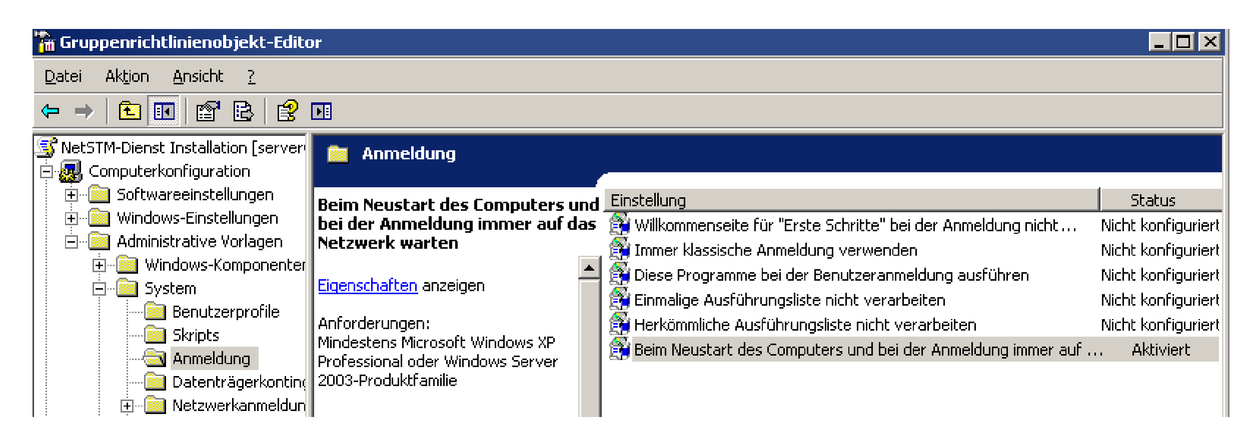
8. Klicken Sie nun auf die Registerkarte **Änderungen**. Fügen Sie die mit ORCA angepasste Datei **custom.mst** hinzu.



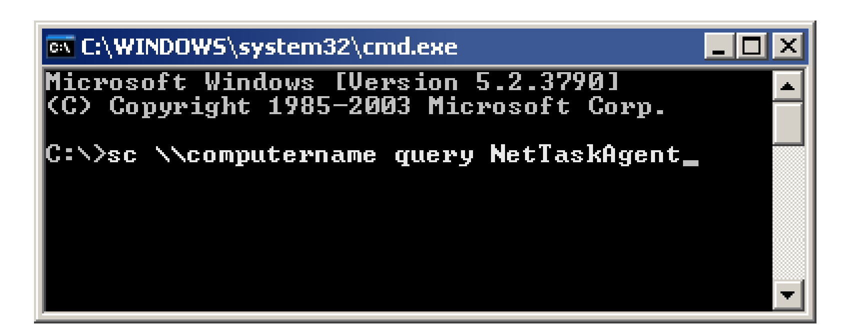
Klicken Sie **OK** und schließen Sie den Gruppenrichtlinienobjekt-Editor.

C) Installation des Dienstes auf den Arbeitsplatzrechnern.

Die ausgewählten Clients der Sicherheitsgruppe "NetSTM-Dienst" installieren den Dienst nun nach ein bis drei Neustarts.
Führen Sie als Administrator auf dem Client den Befehl "gpupdate /Sync" aus oder ändern Sie folgende Gruppenrichtlinie auf Clients, um die Installationsrichtlinie sofort auszuführen:



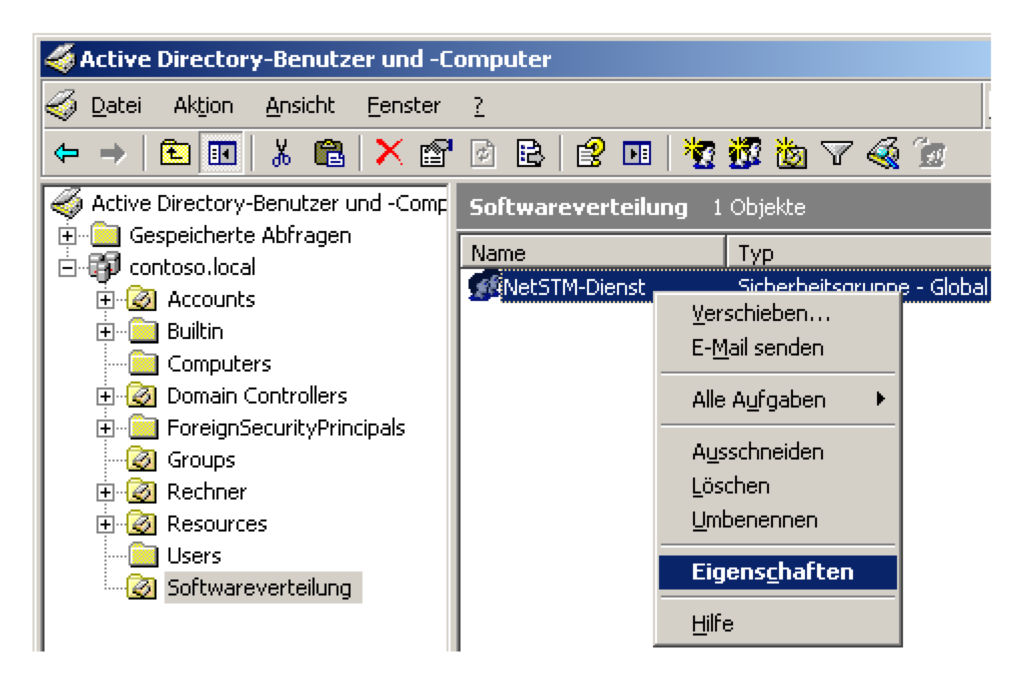
Tipp: Um vom Admin-PC aus zu überprüfen, ob auf einem Client der NetSTM-Dienst läuft, klicken Sie entweder im Computer-Eigenschaften 13 auf Jetzt testen oder führen den Befehl `sc \\clientname query nettaskagent` aus. Hierbei ist ***clientname*** der Computername des Arbeitsplatzrechners im Netzwerk.



Deinstallieren eines MSI-Pakets

Um den Agent-Dienst von einem Client zu deinstallieren, muss man diesen Client wieder aus der Sicherheitsgruppe "NetSTM-Dienst" entfernen.

Hierzu klicken Sie im Startmenü auf Verwaltung > "Active Directory-Benutzer und -Computer". Klicken Sie mit der rechten Maustaste auf die Sicherheitsgruppe "NetSTM-Dienst". Klicken Sie auf **Eigenschaften**.



Klicken Sie anschließend auf die Registerkarte **Mitglieder** und entfernen Sie den gewünschten Computer.

Anmerkung

- Die Deinstallation des MSI-Pakets kann auch mit folgendem Befehl (z.B. in der Eingabeaufforderung oder per Loginscript) gestartet werden:
  `msiexec /x{986222E8-C018-4DA2-94BC-9B796A5A75A5} /qb`
- Als Administrator können Sie auch mit dem Befehl **`NetTaskAgent.exe /u`** oder von einem entfernten Computer aus mit dem Befehl **`sc \\ziel-pc delete nettaskagent`** den Agent-Dienst komplett deinstallieren.
- Mit dem Befehl **`runas /user:administrator cmd`** starten Sie die Eingabeaufforderung mit Administratorrechten (z.B. als Benutzer "Administrator").

Index

- K -

- M -

- N -

- O -

- P -

- Q -

- R -

- S -

- T -

- U -

- V -

- W -

- Z -